The Kronecker-Weber Theorem

Summer School on Cyclotomic fields, Pune, June 7-30, 1999

Eknath Ghate

1 Introduction

These are some brief notes on the famous Kronecker-Weber theorem, which says that cyclotomic extensions of $\mathbb{Q}$ capture *all* abelian extension of $\mathbb{Q}$. Kronecker stated this theorem in 1853, but his proof was incomplete. Weber gave a proof in 1886, but apparently there was still a gap in it. Correct proofs were given soon after by Hilbert and Speiser.

In these notes we shall derive the theorem as a consequence of the theorems of (global) class field theory. The main reference we use is Janusz' book [1]. This is a good first introduction to class field theory - it derives most of the main theorems with minimal use of heavy machinery, and I recommend it to you for further study.

If time permits, I will give another proof of the Kronecker-Weber theorem: namely the one given in Chapter 14 of Washington's book [7]. In this approach, the theorem is deduced from the corresponding statement for local fields, which, in turn, is proved using only 'elementary' facts about the structure of local fields and their extensions. Since the exposition in Washington is good, I will not reproduce this proof in these notes. A word of warning though: one needs to be fairly well acquainted with local fields to enjoy Washington's proof. As an excellent background builder for this, and for many other things, I recommend reading Serre's book [2].

2 Cyclotomic extensions of $\mathbb{Q}$

Let us start by describing what cyclotomic fields, the objects of study of this summer school, look and smell like.

Let ζ_n denote a fixed primitive n^{th} root of unity, and let $\mathbb{Q}(\zeta_n)$ be the number field generated by all the n^{th} roots of unity. The field $\mathbb{Q}(\zeta_n)$ is called the n^{th} cyclotomic field. Most of you have probably already met these fields in the course of working out the proof of the following theorem, which I suggest you now (re-)try and prove for yourself as a warm-up exercise:

Theorem 1 *Let $\phi(n)$ denote the cardinality of $(\mathbb{Z}/n)^\times$. Then $\mathbb{Q}(\zeta_n)$ is an abelian extension of $\mathbb{Q}$ of degree $\phi(n)$. More precisely, there is an isomorphism:*

$$\begin{array}{rcl} (\mathbb{Z}/n)^\times & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ a \pmod n & \mapsto & \sigma_a, \end{array}$$

where $\sigma_a(\zeta_n) = \zeta_n^a$.

Since a sub-extension of an abelian extension is also abelian, cyclotomic fields and their sub-fields already give us an abundant supply of abelian extensions of $\mathbb{Q}$. The obvious question that is now begging to be asked is whether or not there are any more. The answer is a resounding NO!!! More formally, we have the

Theorem 2 (Kronecker-Weber) *Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.*

The rest of these notes will sketch a proof of this beautiful fact using class field theory. But, before we embark on this, let us make a small diversion. At this stage, you may be wondering as to whether every finite abelian group actually occurs as a Galois group of some Galois extension of $\mathbb{Q}$. This is in fact true, and to give you an idea of how one might prove it, let us work out an example.

Let us construct a Galois extension of $\mathbb{Q}$ with Galois group $G = \mathbb{Z}/7 \times \mathbb{Z}/13 \times \mathbb{Z}/13$. The idea is to construct Galois extensions which realize each of the cyclic factors of G. If we can do this in such a way so that these extensions are linearly disjoint, then we have won the game, because we can then just take the compositum of these extensions. So let us first construct an extension with Galois group $\mathbb{Z}/7$. The trick is to choose a prime p such that $p \equiv 1 (\mathrm{mod}\ 7)$. The first prime that works is $p = 29$. Now consider the extension $\mathbb{Q}(\zeta_{29})/\mathbb{Q}$. By Theorem 1, it is an abelian extension with Galois group $\mathbb{Z}/28$. Clearly, since $7|28$, it has a sub-field K_1 whose Galois group is $\mathbb{Z}/7$.

So far so good. We now can similarly construct another extension $K_2/\mathbb{Q}$ with Galois group $\mathbb{Z}/13$. This time we note that $53 \equiv 1 (\text{mod } 13)$, that $\text{Gal}(\mathbb{Q}(\zeta_{53})/\mathbb{Q}) = \mathbb{Z}/52$, and that $13|52$. So the field K_2 with $\text{Gal}(K_2/\mathbb{Q}) = \mathbb{Z}/13$ exists.

Now we have only one more factor to worry about, the 'second' factor of $\mathbb{Z}/13$ in G. This time we choose a different prime congruent to 1 (mod 13). In fact 79 seems to work. As above, in $\mathbb{Q}(\zeta_{79})$ there is a sub-field K_3 with $\text{Gal}(K_3/\mathbb{Q}) = \mathbb{Z}/13$.

Now note that K_1, K_2 and K_3 are linearly disjoint, that is, the intersection of any two of these fields is $\mathbb{Q}$. This is because they each lie in cyclotomic fields $\mathbb{Q}(\zeta_p)$, for different p, which themselves are linearly disjoint. (You could try and use ramification theory to prove this - as a hint note that only p ramifies in $\mathbb{Q}(\zeta_p)$). We now choose $K = K_1K_2K_3$. Then some Galois theory shows $\text{Gal}(K/\mathbb{Q}) = G$, and we are done.

By now, you probably know what to do in general. So why not now try and prove the following theorem:

Theorem 3 *Every finite abelian group is the Galois group of some Galois extension of* $\mathbb{Q}$.

The following interesting fact may come in handy in the course of your proof:

Theorem 4 (Dirichlet) *There are infinitely many primes in every arithmetic progression.*

Now don't be asking whether all finite groups can be realized as Galois groups...! This is one of the hardest problems in mathematics, and is an active area of current research. Let us state it as

Question 1 (Inverse Galois Problem) *Is every finite group the Galois group of a finite Galois extension of* $\mathbb{Q}$*?*

3 Class field theory

Let us now give a short 'proof' of the Kronecker-Weber theorem using class field theory. That this theory should yield a proof at all is hardly surprising, because CLASS FIELD THEORY FOR $\mathbb{Q}$ = THE THEORY OF ABELIAN EXTENSIONS OF $\mathbb{Q}$. However, I should mention up front that

class field theory is a rather broad subject, one that has undergone many re-formulations in terms of both the language and tools it has used to state and prove its main results. To do it justice would require the better part of a year of course work - a time frame somewhat beyond the scope of our five lectures!

Nonetheless, rather than despair, let us be brave, and try and at least get a flavour of some of the statements of the more important theorems of the theory. We shall derive the Kronecker-Weber theorem as an easy consequence of these theorems.

3.1 The Artin Map

The basic object around which most of the statements of class field theory revolve is the Artin map, which has already been introduced by Sury in his lectures. Let us recall its definition.

Let L/K be an abelian extension of number fields. Let I_K denote the group of fractional ideals of K. Let S denote a finite set of prime ideals of K, including all the primes that ramify in L, and let I_K^S denote the subgroup of I_K generated by all the prime ideals outside S. For each fractional ideal $\mathfrak{A}$ in I_K^S, write $\mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$, and set

$$\phi_{L/K}(\mathfrak{A}) = \prod_{\mathfrak{p}} \left[\frac{L/K}{\mathfrak{p}}\right]^{a(\mathfrak{p})}.$$

Here $\left[\frac{L/K}{\mathfrak{p}}\right] \in \mathrm{Gal}(L/K)$ is the Frobenius element at $\mathfrak{p}$. That is, if $\mathfrak{P}$ is a prime of L lying over $\mathfrak{p}$, then $\left[\frac{L/K}{\mathfrak{p}}\right]$ is the element σ in $\mathrm{Gal}(L/K)$ characterized by the property

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}}, \text{ for all } x \text{ in } \mathcal{O}_L\ , \tag{1}$$

where $\mathcal{O}_L$ is the ring of integers of L, and $N(\mathfrak{p})$, the norm of $\mathfrak{p}$, is the cardinality of the residue field of $\mathfrak{p}$.

The homomorphism $\phi_{L/K} : I_K^S \to \mathrm{Gal}(L/K)$ is called the Artin map for the extension L/K. The first deep theorem about it is:

Theorem 5 *The Artin map $\phi_{L/K}$ is surjective.*

We shall not say anything about the proof of this theorem, except that one possible approach to it is, funnily enough, via analysis (L-Series and Density Theorems are catchwords here).

Another important theorem that we shall need, that can also be established by analytic methods, is the following:

Theorem 6 *Let L_1 and L_2 be two finite Galois (not necessarily abelian) extensions of K, and let S_1 and S_2 denote the sets of primes of K which split completely in L_1 and L_2 respectively. Then $S_1 \subset S_2$ (except for a set of density 0) if and only if $L_2 \subset L_1$.*

Again, we shall not define what it means for a set of primes to have density 0; suffice it to say that sets of finite cardinality have density 0, and it is only such exceptional sets that will appear in the application we have in mind below.

3.2 The kernel of $\phi_{L/K}$

One of the aims of class field theory is to describe the kernel of the Artin map explicitly. Note that a prime ideal $\mathfrak{p} \in \ker \phi_{L/K}$ if and only if the Frobenius element at $\mathfrak{p}$ is trivial, that is:

$$\left[\frac{L/K}{\mathfrak{p}}\right] = 1.$$

Since you know that the Frobenius element has order $f(\mathfrak{P}/\mathfrak{p})$, the residue degree of $\mathfrak{P}|\mathfrak{p}$, we see that, in this case, both $e(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}) = 1$. This forces $g(\mathfrak{P}/\mathfrak{p}) = [L : K]$, which is to say that $\mathfrak{p}$ splits completely in the extension L/K. Thus, apart from a finite set of primes, the primes in the kernel of the Artin map are exactly the primes that split completely.

Definition 1 *A* modulus *for K is a formal product*

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$$

taken over all primes (including the infinite primes) of K. The exponents $n(\mathfrak{p})$ are non-negative integers, and are positive for only a finite number of $\mathfrak{p}$. Furthermore $n(\mathfrak{p}) = 0$ or 1 when $\mathfrak{p}$ is real, and $n(\mathfrak{p}) = 0$ when $\mathfrak{p}$ is complex.

A modulus $\mathfrak{m}$ may be written as $\mathfrak{m}_f\mathfrak{m}_\infty$, where the first (resp. second) factor is divisible only by the finite (resp. infinite) places. Now let $\mathcal{O}_K$ denote the ring of integers of K. Set

$$\begin{aligned} K_{\mathfrak{m}} &= \{a/b \mid a, b \in \mathcal{O}_K, (a), (b) \text{ relatively prime to } \mathfrak{m}_f\}, \\ K_{\mathfrak{m},1} &= \{\alpha \in K_{\mathfrak{m}} \mid \alpha \equiv 1 \pmod{\mathfrak{m}}\} \end{aligned}$$

Here the condition $\alpha \equiv 1 \pmod{\mathfrak{m}}$ means the following: for each finite $\mathfrak{p}$ dividing $\mathfrak{m}_f$, we require that $v_{\mathfrak{p}}(\alpha - 1) \geq n(\mathfrak{p})$, and for each real prime $\mathfrak{p}$ dividing $\mathfrak{m}_\infty$, we require α to be positive at this place.

Write $I_K^{\mathfrak{m}}$ for the group I_K^S where S is the set of primes dividing $\mathfrak{m}_f$. We assume that $\mathfrak{m}_f$ is divisible by all the finite primes that ramify in L. Note that, via the map $x \mapsto (x)$, $K_{\mathfrak{m},1}$ may be thought of as a subgroup of $I_K^{\mathfrak{m}}$.

Definition 2 *The quotient*

$$\frac{I_K^{\mathfrak{m}}}{K_{\mathfrak{m},1}}$$

is called the ray class group *modulo* $\mathfrak{m}$. *Note that when* $\mathfrak{m} = 1$ *this is just the usual* class group *of* K.

Each prime in K may also be viewed as a product of primes in L. In this way $\mathfrak{m}$ may also be considered as a modulus for L, and so it makes sense to speak of the group $I_L^{\mathfrak{m}}$. Moreover, there is a natural norm map

$$\begin{aligned} N_{L/K} : I_L^{\mathfrak{m}} &\to I_K^{\mathfrak{m}}, \\ \mathfrak{P} &\mapsto \mathfrak{p}^f, \end{aligned}$$

where $f = f(\mathfrak{P}/\mathfrak{p})$. The first approximation to the kernel of the Artin map is given by the following proposition:

Proposition 1 *Let* L/K *be a finite abelian extension, and let* $\mathfrak{m}$ *be any modulus of* K *such that* $\mathfrak{m}_f$ *is divisible by all the primes of* K *which ramify in* L. *Then* $N_{L/K}(I_L^{\mathfrak{m}}) \subset \ker \phi_{L/K}$.

Proof: This follows immediately from the fact that the Artin map maps $\mathfrak{p}^f$ to $\left[\frac{L/K}{\mathfrak{p}}\right]^f = 1$.

The following key theorem now tells us exactly what the 'missing part' of the kernel of the Artin map is.

Theorem 7 (Artin Reciprocity Theorem) *Let L/K be a finite abelian extension. Then there exists a modulus $\mathfrak{m}$ divisible by at least the primes of K which ramify in L such that the kernel of the Artin map is given by:*

$$\ker \phi_{L/K} = N_{L/K}(I_L^{\mathfrak{m}}) \cdot K_{\mathfrak{m},1}. \tag{2}$$

Let us say that the modulus $\mathfrak{m}$ *divides* $\mathfrak{m}'$ (and write $\mathfrak{m}|\mathfrak{m}'$) if each place that occurs in $\mathfrak{m}$ occurs in $\mathfrak{m}'$ with equal or larger exponent. It is a fact that if (2) holds for $\mathfrak{m}$ then it holds for all moduli $\mathfrak{m}'$ which are divisible by $\mathfrak{m}$. So the following definition is rather natural:

Definition 3 *The greatest common divisor of all the moduli $\mathfrak{m}$ such that* (2) *holds is called the* conductor *of L/K.*

Note: It is not clear that, so defined, the conductor of L/K is divisible by all the ramified primes, but this is in fact true.

3.3 An example

It is about time that we gave an example to illustrate the above concepts. What better place to start than with cyclotomic fields? So let us set $K = \mathbb{Q}$, and $L = \mathbb{Q}(\zeta_n)$, for some fixed n.

We will show that the Artin reciprocity theorem (Theorem 7) holds for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ with the modulus $\mathfrak{m} = n \cdot \infty$, where ∞ is the unique real infinite place of $\mathbb{Q}$. We must include ∞ in the modulus since ∞ ramifies in the totally imaginary field $\mathbb{Q}(\zeta_n)$.

Let p be a prime not dividing n. Then the ideal (p) is unramified in L. Moreover, σ_p (see Theorem 1 for notation) satisfies the condition (1) characterizing the Frobenius at p, so we see that $\phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(p) = \sigma_p$. This shows that for any two positive integers a and b relatively prime to n,

$$\phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(a/b) = \sigma_{ab^*}, \tag{3}$$

where b^* is a positive integer prime to n with $bb^* \equiv 1 (\mathrm{mod}\ n)$. This formula allows us to compute the kernel of the Artin map. Indeed, we may easily compute that

$$\ker \phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} = \{(a/b) \mid a, b \text{ positive}, a \equiv b \ (\mathrm{mod}\ n)\} = \mathbb{Q}_{\mathfrak{m},1}. \tag{4}$$

The surjectivity of the Artin map is of course something we are assuming (see Theorem 5). But note that in this case the surjectivity is essentially equivalent to Dirichlet's theorem that there are infinitely many primes in every arithmetic progression (see Theorem 4).

Putting things together, we see that the Artin map induces an isomorphism between the ray class group modulo $\mathfrak{m} = n \cdot \infty$, and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n)^\times$.

As it turns out $\mathfrak{m} = n \cdot \infty$ is in fact the greatest common divisor of all the moduli such that (2) above holds, and so it is also the conductor of the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

3.4 The Kronecker-Weber theorem

We can now derive the Kronecker-Weber theorem. We need one last result:

Proposition 2 *Let L/K be an abelian extension and $\mathfrak{m}$ a modulus so that (2) above holds. Let E/K be an arbitrary Galois extension such that*

$$N_{E/K}(I_E^{\mathfrak{m}}) \subset N_{L/K}(I_L^{\mathfrak{m}}) \cdot K_{\mathfrak{m},1}. \tag{5}$$

Then $L \subset E$.

Proof: Say $\mathfrak{p}$ is a prime of K that does not divide $\mathfrak{m}_f$. Then, if $\mathfrak{p}$ splits completely in E, it is trivially the norm of a prime of E, and so $\mathfrak{p} \in N_{E/K}(I_E^{\mathfrak{m}})$. By (5) and Theorem 7 above, we see that $\mathfrak{p} \in \ker \phi_{L/K}$, so that $\mathfrak{p}$ splits completely in L. We now apply Theorem 6 to see that $L \subset E$.

Proof of Kronecker-Weber: Say that L is an arbitrary abelian extension of $\mathbb{Q}$. We want to show that $L \subset \mathbb{Q}(\zeta_n)$, for some n. Now Theorem 7, applied to L, yields a modulus $\mathfrak{m}$ over $\mathbb{Q}$ such that (2) holds. We may suppose that $\mathfrak{m} = n \cdot \infty$, for some n. Now set $E = \mathbb{Q}(\zeta_n)$. Then, by (4), $\ker \phi_{E/\mathbb{Q}} = \mathbb{Q}_{\mathfrak{m},1}$ and so

$$N_{E/\mathbb{Q}}(I_E^{\mathfrak{m}}) \subset N_{E/\mathbb{Q}}(I_E^{\mathfrak{m}}) \cdot \mathbb{Q}_{\mathfrak{m},1} = \mathbb{Q}_{\mathfrak{m},1} \subset N_{L/\mathbb{Q}}(I_L^{\mathfrak{m}}) \cdot \mathbb{Q}_{\mathfrak{m},1} = \ker \phi_{L/\mathbb{Q}}.$$

By Proposition 2, we obtain $L \subset E = \mathbb{Q}(\zeta_n)$ as desired.

3.5 Existence theorem

Though we have now 'proved' the Kronecker-Weber theorem, let us pick up some loose ends and round off our whirlwind survey of class field theory. We return to the general situation: L/K will denote an abelian extension of number fields.

Note that if $K \neq \mathbb{Q}$, then so far, no part of the discussion above guarantees the existence of even one abelian extension L of K! This is remedied by the following:

Theorem 8 (Existence Theorem) *Let $\mathfrak{m}$ be a modulus. Then there exists a finite abelian extension L/K, such that every prime of K that ramifies in L occurs in $\mathfrak{m}_f$, and such that* (2) *above holds.*

This modulus $\mathfrak{m}$ may not be the conductor of the extension L/K, but by definition, the conductor certainly divides it. Also, curiously, some moduli may never be conductors at all (example: $\mathfrak{m} = \infty$ is never the conductor of any finite abelian extension of $\mathbb{Q}$). However, once a modulus $\mathfrak{m}$ occurs as a conductor, it is a fact that there is a maximal finite abelian extension, $L_{\mathfrak{m}}$, having $\mathfrak{m}$ as its conductor. It turns out that in this case $\ker \phi_{L_{\mathfrak{m}}/K} = K_{\mathfrak{m},1}$.

Definition 4 *$L_{\mathfrak{m}}$ is called the* ray class field *of conductor $\mathfrak{m}$.*

Note that via the Artin map, the Galois group of the ray class field of conductor $\mathfrak{m}$ is just the ray class group modulo $\mathfrak{m}$. Also note that every abelian extension L of K sits inside a ray class field, namely the one whose conductor is the conductor of L. Finally, in the case when $K = \mathbb{Q}$ (see Section 3.3), we see that the cyclotomic fields are the ray class fields (of conductor $\mathfrak{m} = n \cdot \infty$).

3.6 Classification theorem

We now wish to state the climactic theorem of class field theory - the Classification theorem - which says roughly that the abelian extensions L of K are parameterized by gadgets constructed purely out of K! Let us make some preliminary definitions:

Definition 5 *A group H is said to be a* congruence subgroup of level $\mathfrak{m}$ *if it satisfies*

$$K_{\mathfrak{m},1} \subset H \subset I_K^{\mathfrak{m}},$$

for some modulus $\mathfrak{m}$.

The key example of a congruence subgroup of course is the following: if L/K is a finite abelian extension of K, then the Artin reciprocity theorem says that $H = \ker \phi_{L/K}$, is a congruence subgroup of level $\mathfrak{m}$ for some modulus $\mathfrak{m}$.

To rid us of the somewhat unpleasant dependence on the modulus $\mathfrak{m}$, we now put an equivalence relation $\sim$ on the set of congruence subgroups.

But first let us make a remark. Let $\mathfrak{m}$ and $\mathfrak{m}'$ be two moduli, with $\mathfrak{m}'|\mathfrak{m}$. Then $I_K^{\mathfrak{m}}$ is a subgroup of $I_K^{\mathfrak{m}'}$. If H' is a congruence subgroup of level $\mathfrak{m}'$ then there may or may not be a congruence subgroup H of level $\mathfrak{m}$ such that $H = I_K^{\mathfrak{m}} \cap H'$. If this does happen then we say that the congruence subgroup H is the restriction of the congruence subgroup H'.

Now say $(H_1, \mathfrak{m}_1)$ and $(H_2, \mathfrak{m}_2)$ are two congruence subgroups. We set $H_1 \sim H_2$, if there exists a modulus $\mathfrak{m}$, with $\mathfrak{m}_i \,\big|\, \mathfrak{m}$, for $i = 1, 2$, and so that $I_K^{\mathfrak{m}} \cap H_1 = I_K^{\mathfrak{m}} \cap H_2$ as restricted congruence subgroups of level $\mathfrak{m}$.

Definition 6 *An* ideal group $[H]$ *is an equivalence class of congruence subgroups* $(H, \mathfrak{m})$ *with respect to the equivalence relation* $\sim$.

The ideal groups are the 'gadgets' referred to above which parameterize abelian extensions of K. In fact we have:

Theorem 9 (Classification Theorem) *The map*

$$L/K \quad \mapsto \quad [\ker \phi_{L/K}]$$

is an inclusion reversing bijection between the set of abelian extensions L *of* K *and the set of ideal groups of* K.

Here 'inclusion reversing' means that if the abelian extensions L_1 and L_2 correspond to the ideal groups $[H_1]$ and $[H_2]$ respectively, then

$$L_1 \subset L_2 \iff [H_2] \subset [H_1].$$

(Note: $[H_2] \subset [H_1]$ simply means that there are congruence subgroups $H \in [H_2]$ and $H' \in [H_1]$ of the same level such that $H \subset H'$; one needs to check that this is well defined).

3.7 Hilbert class field

There is one particular ray class field that is the simplest and most important. This is the Hilbert class field. It is defined to be the ray class field of conductor $\mathfrak{m} = 1$. We shall denote it by U. The following theorem now follows easily, after the discussion above.

Theorem 10 *The Hilbert class field U is the maximal finite everywhere unramified abelian extension of K. Moreover, the Artin map establishes an isomorphism between the class group of K and $\mathrm{Gal}(U/K)$. In particular the class number of K is just $[U : K]$.*

As a consequence of this theorem we see that a prime $\mathfrak{p}$ of K splits completely in U if and only if it is a principal ideal of K. This is not to be confused with the following theorem, which was proved by Furtwangler.

Theorem 11 (Principal Ideal Theorem) *Every ideal of K becomes principal in U.*

Obviously, the Hilbert class field of $\mathbb{Q}$ is just $\mathbb{Q}$ itself, since $\mathbb{Q}$ has class number 1. But the above theorems show that the Hilbert class field for a number field with non-trivial class number is a very interesting object. We shall say a little more about the Hilbert class field of an imaginary quadratic situation in the next section.

3.8 Complex multiplication

We have seen that the ray class field of $\mathbb{Q}$ of conductor $\mathfrak{m} = n \cdot \infty$ is exactly the cyclotomic field $\mathbb{Q}(\zeta_n)$, and that every abelian extension of $\mathbb{Q}$ sits in one of these ray class fields. This is indeed a very satisfying result since we can generate *explicitly* all the abelian extension of $\mathbb{Q}$ by values of the exponential function $e^{2\pi iz}$ at certain division points $z \in \mathbb{Q}/\mathbb{Z}$.

A central problem in class field theory is to be able to similarly generate the abelian extensions of an arbitrary number field by values of transcendental functions. In fact this problem has its origins in Kronecker's famous 'Jugendtraum' (= youthful dream, in German).

When K is an imaginary quadratic field, this problem has been completely solved by the so called theory of 'complex multiplication'. Essentially the idea is that the ray class fields are generated by values of the famous j function at

points in the imaginary quadratic field K, as well as by values of the Weber function w, at division points of an elliptic curve with complex multiplication by K. It would take us too far afield from the purpose of these notes to make this any more precise. However, to get our toes wet, let us at least describe how to generate the Hilbert class field of K.

For each $z \in \mathbb{C}$ with positive imaginary part, let $j(z)$ be the corresponding value of the elliptic modular function, defined by

$$j(z) = 1728 \cdot \frac{g_2(z)^3}{g_2(z)^3 - 27g_3(z)^2},$$

where

$$g_2(z) = 60 \sum_{(0,0)\neq(m,n)\in\mathbb{Z}^2} \frac{1}{(mz+n)^4},\ g_3(z) = 140 \sum_{(0,0)\neq(m,n)\in\mathbb{Z}^2} \frac{1}{(mz+n)^6}.$$

Then we have the beautiful theorem:

Theorem 12 *Let Let K be an imaginary quadratic field, with ring of integers $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\tau$. Then $j(\tau)$ is an algebraic integer, and $U = K(j(\tau))$ is the Hilbert class field of K.*

3.9 Hilbert's twelfth problem

The generation of ray class fields by the values of transcendental functions was emphasized by Hilbert in his 'twelfth problem' presented at the Paris International Congress of Mathematicians in 1900. He wrote

> "The extension of Kronecker's theorem to the case that in place of the realm of rational numbers or of the imaginary quadratic field any algebraic field whatever is laid down as realm of rationality, seems to me of the greatest importance. I regard this problem as one of the most profound and far reaching in the theory of numbers and of functions."

So far very little progress has been made on the problem in general. However, in closing these notes, let us at least mention some additional special cases that have been partially treated:

3.9.1 CM fields

From the point of view of 'complex multiplication' the most natural way to to generalize the results obtained for imaginary quadratic fields is to replace elliptic curves by higher dimensional abelian varieties. This was done by Shimura and Taniyama, who managed to generate class fields of 'CM fields'. A CM field is the higher analog of an imaginary quadratic field: it is a totally imaginary quadratic extensions of a totally real field. It must be pointed out that unfortunately not all abelian extension of CM fields can be generated by this method.

Shimura and Taniyama's theory is exposed in their book [5]. There is also a new edition, [4], now on the market.[1]

See also Wafa Wei's (unpublished) thesis, where she gives some information about the maximal abelian extension of a CM field that can be generated by the values of automorphic functions [8].

3.9.2 Real quadratic fields

Some partial results have been obtained by Shimura in this case using abelian varieties with real multiplication. For more details see the last chapter of his book [3].

3.9.3 Stark's method

Another approach to Hilbert's twelfth problem has been proposed by Stark, who has shown that certain abelian extensions of arbitrary number fields can be generated by the values of Artin L-functions at $s = 0$. You could look at Tate's efficient monograph [6] for more details.

References

[1] G. Janusz. *Algebraic number fields.* Academic Press, New York-London, 1973.

[1] In the preface to [5] it was claimed that Hecke had shown how to generate class fields of certain CM bi-quadratic extensions of $\mathbb{Q}$ by values of Hilbert modular functions. Apparently this work of Hecke was not complete (see the preface to [4]), but in any case, has since been corrected and subsumed by the work [4].

[2] J.-P. Serre. *Local fields, GTM 67.* Springer-Verlag, Berlin-New York, 1979.

[3] G. Shimura. *Introduction to the arithmetic theory of automorphic functions.* Princeton Univ. Press, Princeton, 1971.

[4] G. Shimura. *Abelian varieties with complex multiplication and modular functions, Princeton Mathematical Series, 46.* Princeton Univ. Press, Princeton, 1999.

[5] G. Shimura and Y. Taniyama. *Complex multiplication of abelian varieties and its applications to number theory, Publications of the Mathematical Society of Japan, 6.* The Mathematical Society of Japan, Tokyo, 1961.

[6] J. Tate. *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$.* Birkhäuser, 1984.

[7] L. Washington. *Introduction to cyclotomic fields, Second edition.* Springer-Verlag, Berlin-New York, 1996.

[8] W. Wei. Moduli fields of CM-motives applied to Hilbert's 12th problem. *Preprint, Available on the world wide web at http://www.mathematik.uni-bielefeld.de/sfb343/preprints/pr94070.ps.gz*, 1994.