Class Field Theory : Proofs and Applications

Daniel Fretwell

October 9, 2013

Contents

1 Introduction

This document is a continuation of my Semester 1 project on class field theory. In the previous work, we made a rounded exposition of the fundamentals of class field theory but in order to preserve the document length the main proofs had to be skipped. We concentrate on filling in the gaps in this second installment. Due to the need to complete the arguments left open last semester and the need for applications this part of the project is a little longer than it should have been.

It was not mentioned in the previous project but the class field theory we are studying here is *global* class field theory. There is such a thing as *local* class field theory in which we study the Abelian extensions of local fields (essentially fields that arise as completions of a number field with respect to places). Actually we touch on these ideas slightly in this project but never quite get to defining a local Artin map and looking at the local analogues of the main theorems of global class field theory. For those wanting to continue on to study local class field theory, consider Chapter 7 of [2]

To start off this project we shall first restate the main definitions and theorems. This will be brief and those wanting to remind themselves of the details should consult my Semester 1 project. There will be very little motivation or technical results here since this was the purpose of the work done previously.

We then set out to prove the main theorems of class field theory. With our present knowledge this would not be a simple task and we soon find that we first have to invent or discover new concepts such as the

idele group and the corresponding *idele class group*. These are topological devices that take stock of all completions of a number field at once. Such constructions will make the theory much easier to understand and formulate, whilst at the same time generalising the theory to all Abelian extensions. The cohomology of finite Abelian groups will be introduced and used alongside the idele theory to establish an important inequality. We use L-series in conjunction with the ideal theory to establish another important inequality. Combining the two inequalities will give a nice result that allows us to prove Artin reciprocity.

In order to prove the existence theorem we resort to using Kummer n-extensions and the notion of a class field. This middle chunk of the project will be quite technical but hopefully enjoyable and illuminating. The books by Lang [1] and Childress [2] will be invaluable for this part of the work.

Finally, we shall consider an application of the theory. We use class field theory to provide a partial answer to the question:

$$\text{Given } n \in \mathbb{N}, \text{ which rational primes can be written in the form } x^2 + ny^2 \text{ for some } x, y \in \mathbb{Z}?.$$

The question will only be answered here in the case of square-free n satisfying $n \not\equiv 3 \bmod 4$.

Although class field theory can be used to answer this question in full it is only a theoretical answer, depending on knowledge of a specific generator for the Hilbert class field of the number field $\mathbb{Q}(\sqrt{-n})$. To get a practical answer we would need to be able to find this Hilbert class field for each n by some explicit method rather than by clever guesswork. This is a difficult thing to do and is beyond the scope of this project but can be done by using *j-invariants* of elliptic curves with certain complex multiplication.

To round off the project a brief discussion will be made detailing the solution to this problem for all n and how class field theory still manages to provide an answer. We follow Cox [3] with this nice application of class field theory.

Before embarking on our journey I have decided to make a passing mention of other major uses of class field theory that could not be studied in detail in my project.

The Cebotarev density theorem is a simple corollary of class field theory that tells us interesting information about how prime ideals are distributed amongst ideal classes. This theorem provides Dirichlet's theorem on primes in arithmetic progressions as an easy corollary (in fact it is just a specific case of the theorem). The Cebotarev density theorem is stated and proved on p.169 of [1].

Also, by use of the Artin reciprocity law we can recover so called higher reciprocity laws that generalise the quadratic, cubic and quartic reciprocity laws of Gauss. Historically speaking, the Artin reciprocity law was successfully created out of an attempt at unifying all of these reciprocity laws. It provided a partial solution to Hilbert's ninth problem in that it creates a general reciprocity law but one that only works with the Abelian extensions of a given number field. To see these links of Artin reciprocity with higher reciprocity see p.165-p.168 of [3]. For those wanting to see higher reciprocity laws arise in chronological order (before class field theory) I recommend [6] for a detailed read with lots of concrete results.

2 Reminder of global class field theory

As mentioned in the introduction, this section is to serve as a brief reminder of the global class field theory that we studied previously. The reader may skip this section if desired.

2.1 Underlying theory

We defined a *modulus* $\mathfrak{m}$ of a number field K to be a formal product of prime ideals of $\mathfrak{O}_K$ and distinct real embeddings of K. The ideal part of $\mathfrak{m}$ was referred to as the *finite part* and was denoted $\mathfrak{m}_0$. The real embedding part of $\mathfrak{m}$ was referred to as the *infinite part* and was denoted $\mathfrak{m}_\infty$.

This object allowed us to, in some sense, choose the entire ramification that we would like a given Abelian extension to have. We did this by constructing the groups $I_K(\mathfrak{m})$ and $P_K(\mathfrak{m})$, consisting of fractional ideals (and principal fractional ideals respectively) of K that are coprime to $\mathfrak{m}$. These groups were to represent the ideals that were not divisible by any of the prime ideals we had identified in choosing the modulus $\mathfrak{m}$. This can be thought of as avoiding the ramification decided by $\mathfrak{m}$.

We then considered the subgroup $P_{K,1}(\mathfrak{m})$ of $P_K(\mathfrak{m})$ consisting of those principal fractional ideals (α) with generator $\alpha \in K^\times$ satisfying $\alpha \equiv 1 \bmod \mathfrak{m}_0$ and $\sigma(\alpha) > 0$ for all real embeddings σ in $\mathfrak{m}_\infty$.

Given any modulus $\mathfrak{m}$ of a number field K we called any group H such that $P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m})$ a *congruence subgroup* for $\mathfrak{m}$ and called the quotient group $I_K(\mathfrak{m})/H$ a *generalised ideal class group* for $\mathfrak{m}$. We will prove later that these generalized ideal classes are finite for any modulus.

It was our aim in developing class field theory to connect the generalised ideal class groups with the Abelian extensions of K, in order to classify all possible Abelian extensions of K. This connection meant that certain data *extrinsic* to K (the Abelian extensions of K) could be found entirely in terms of certain data *intrinsic* to K (the generalised ideal class groups). We actually saw that we could develop a one-to-one correspondence with the use of the Artin map. We pause to remind ourselves of this map.

2.2 The Artin map

Recall that in any finite Galois extension L/K of number fields the Galois group $\mathrm{Gal}(L/K)$ acts transitively on the prime ideals $\mathcal{P}_i$ of $\mathfrak{O}_L$ lying above a given prime ideal $\mathfrak{p}$ in $\mathfrak{O}_K$ (in other words the prime ideals that occur in the prime ideal factorisation of $\mathfrak{p}\mathfrak{O}_L$ in $\mathfrak{O}_L$). Given such a $\mathcal{P}_i$ we defined the *decomposition group* $D_{\mathcal{P}_i/\mathfrak{p}}$ to be the stabilizer of $\mathcal{P}_i$ under this action. We also considered the elements in the decomposition group that induce automorphisms fixing the residue field $\mathfrak{O}_L/\mathcal{P}_i$ and came up with the *inertia group* $I_{\mathcal{P}_i/\mathfrak{p}}$.

There turned out to be a canonical epimorphism between $D_{\mathcal{P}_i/\mathfrak{p}}$ and $\mathrm{Gal}((\mathfrak{O}_L/\mathcal{P}_i)/(\mathfrak{O}_K/\mathfrak{p}))$ with kernel $I_{\mathcal{P}_i/\mathfrak{p}}$, thus providing an isomorphism:

$$D_{\mathcal{P}_i/\mathfrak{p}}/I_{\mathcal{P}_i/\mathfrak{p}} \cong \mathrm{Gal}((\mathfrak{O}_L/\mathcal{P}_i)/(\mathfrak{O}_K/\mathfrak{p})).$$

When $\mathfrak{p}$ is unramified in L, we saw that the inertia group is trivial (and conversely too). Thus in the unramified case we had the isomorphism:

$$D_{\mathcal{P}_i/\mathfrak{p}} \cong \mathrm{Gal}((\mathfrak{O}_L/\mathcal{P}_i)/(\mathfrak{O}_K/\mathfrak{p})).$$

The group on the right here is cyclic, generated by a Frobenius automorphism (since the extension $(\mathfrak{O}_L/\mathcal{P}_i)/(\mathfrak{O}_K/\mathfrak{p})$ is isomorphic to an extension of finite fields). Thus when $\mathfrak{p}$ is unramified in L there had to exist, for each $\mathcal{P}_i$, a unique generator for $D_{\mathcal{P}_i/\mathfrak{p}}$ that is mapped to this Frobenius automorphism under the above isomorphism. These generators were called *Artin symbols*, denoted by $\left(\frac{L/K}{\mathcal{P}_i}\right)$ and there was one corresponding to each $\mathcal{P}_i$.

When the finite extension L/K considered was Abelian we found that the Artin symbols coincided for all choices of $\mathcal{P}_i$ meaning that we could define the Artin symbol here as $\left(\frac{L/K}{\mathfrak{p}}\right)$, i.e. as if the Artin symbol here is really something belonging to $\mathfrak{p}$. Further, in this case we could extend the definition of Artin symbol in a multiplicative way to be defined on fractional ideals of K (as long as none of the fractional ideals used had any prime ideal divisors that were ramified in L). To take account for this we introduced the notion of a *complete modulus* for L/K, namely one that has finite part containing all prime ideals of $\mathfrak{O}_K$ that ramify in L.

So given a finite Abelian extension L/K and any complete modulus $\mathfrak{m}$, we have a well defined group homomorphism:

$$\Phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K).$$

This is the so called *Artin map*, which I may also denote as $\left(\frac{L/K}{\cdot}\right)$ when the modulus we are using is understood.

Now the main theorems of class field theory can be presented again for the reader.

2.3 The main theorems

The details of the one to one correspondence are given by the following two theorems. It is these theorems which we aim to prove in this part of the project. This will not be an easy task and will take up most of the project, although in proving these theorems we will discover a lot of nice mathematics.

Recall that we defined a relative norm function:

$$N_{L/K} : I_L(\mathfrak{m}) \longrightarrow I_K(\mathfrak{m}),$$

which is completely defined by the fact that it sends any prime ideal $\mathcal{P}$ of $\mathfrak{O}_L$, not dividing $\mathfrak{m}_0$, to $\mathfrak{p}^f$, where $f = [\mathfrak{O}_L/\mathcal{P} : \mathfrak{O}_K/\mathfrak{p}]$ and $\mathfrak{p}$ is the unique prime ideal of $\mathfrak{O}_K$ that lies below $\mathcal{P}$. This relative norm function is a group homomorphism.

Theorem 2.3.1. *(The Artin Reciprocity Theorem) Given a finite abelian extension L/K of a number field K we have that:*

1. *the Artin map $\Phi_{L/K,\mathfrak{m}}$ is a surjection for any complete modulus $\mathfrak{m}$ of L/K,*
2. *if the exponents of the prime ideals in the complete modulus $\mathfrak{m}$ are made big enough then $\ker(\Phi_{L/K,\mathfrak{m}})$ becomes a congruence subgroup for $\mathfrak{m}$ (in other words $P_{K,1}(\mathfrak{m}) \subseteq \ker(\Phi_{L/K,\mathfrak{m}})$).*

   More specifically, for such moduli we have that $\ker(\Phi_{L/K,\mathfrak{m}}) = P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$, thus giving the isomorphism:

   $$I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m})) \cong \mathrm{Gal}(L/K),$$

   so there exists a corresponding generalised ideal class group for the Abelian extension L/K.

This theorem is mightily important since not only does it form the correspondence one way but it also gives the exact kernel of the Artin map in an explicit form, allowing us to form the corresponding generalised ideal class group. In future I shall refer to the kernel of the Artin map as the *Artin kernel* for simplicity.

There is a unique "smallest" complete modulus that makes the above isomorphism work. This best choice of modulus is called the *conductor*. This notion was discussed briefly in part one of this project but we will discuss this in more detail later.

So the Artin reciprocity theorem sets in stone the correspondence one way. Given an Abelian extension L/K, we know a lot about the group $\mathrm{Gal}(L/K)$ and along with the existence of this special modulus, the conductor, we can find a corresponding generalised ideal class group. This is done via the Artin map and the Artin kernel.

The other direction of the correspondence is given by the following:

Theorem 2.3.2. *(The Existence Theorem) Let $\mathfrak{m}$ be any modulus of a number field K. Then for each congruence subgroup H for $\mathfrak{m}$ there exists a unique Abelian extension L/K with H as its Artin kernel. Further, we have that $\mathfrak{m}$ is a complete modulus for the extension L/K.*

Thus for each congruence subgroup H for $\mathfrak{m}$, there exists a number field L such that L/K is Abelian and:

$$I_K(\mathfrak{m})/H \cong \mathrm{Gal}(L/K).$$

The one-to-one correspondence is now apparent. We will get to see proofs of these theorems in Section 4 and we will see an application of the correspondence in Section 5 when we construct the Hilbert class field of K.

Our general strategy in proving Artin reciprocity will be to obtain the important equality:

$$[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})N_{L/K}(\mathfrak{m})] = [L : K],$$

for cyclic extensions L/K and a certain type of modulus $\mathfrak{m}$. Then we will use surjectivity of the Artin map (which can be proved easily) to prove the rest of the Artin reciprocity law. Of course this will only prove Artin reciprocity for the cyclic case. The general case where L/K is an Abelian extension will be produced as an easy corollary.

However, getting the above equality requires two inequalities to be proved. The universal norm index inequality will establish that:

$$[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})N_{L/K}(\mathfrak{m})] \leq [L : K],$$

for any Abelian extension L/K and any modulus $\mathfrak{m}$ of K. Proof of this will require L-series.

The global cyclic norm index inequality will give us the other direction:

$$[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})N_{L/K}(\mathfrak{m})] \geq [L : K],$$

but we are only able to prove this for cyclic extensions and special kinds of moduli. Proof of this will require ideles and cohomology.

The proof of the existence theorem will depend on Kummer n-extensions. These are special field extensions such that the base field contains the n-th roots of unity and such that the Galois group has a special condition (also depending on n).

3 The path to the idelic view

The version we have of class field theory is quite messy to visualise as it stands. Proving the theorems using only this view is not an easy task (although possible).

In this section we construct a new set of objects, the ideles, with which we can make class field theory much nicer to study. Not only does the theory appear more concise when viewed with these global objects but also the ideles generalise the theory to include all Abelian extensions (not necessarily finite ones).

I assume the reader knows about places of a number field and the corresponding completion fields (i.e. mostly $\mathfrak{p}$-adic fields). If the reader is not familliar with such things then Chapter 2 of [1] has all of the necessary material. I reference this section due to the limitations in length of this project.

3.1 Ideles

As usual we start with a number field K. As we know, there are infinitely many completions of K and they are classified corresponding to the places of K.

The finite places each give a $\mathfrak{p}$-adic completion for some prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$, which we denote $K_\mathfrak{p}$ (when a specific $\mathfrak{p}$ is considered). The infinite places each give a completion isomorphic to either $\mathbb{R}$ or $\mathbb{C}$, depending on the nature of the place (real infinite or complex infinite respectively).

The ideles that we are about to introduce are going to give us a way to look at all completions at once rather than having to focus on one particular completion at a time. The construction is going to be close to that of the direct product of the completions, but is an example of a *restricted direct product*.

Firstly, denote the completion of K with respect to a given place v by K_v. When v is finite we let $\mathfrak{O}_v$ denote the ring of elements of K_v that have absolute value less than or equal to 1 (under the corresponding $\mathfrak{p}$-adic absolute value in v). Then $\mathfrak{O}_v^\times$ is the set of elements in $\mathfrak{O}_v$ that have absolute value 1. In fact, when we deal with a finite place v we let $\mathfrak{p}_v$ denote the prime ideal of $\mathfrak{O}_K$ that it corresponds to.

Definition 3.1.1. Define the *unit group* U_v to be $\mathfrak{O}_v^\times$ when v is finite, $\mathbb{R}^\times$ when v is real infinite and $\mathbb{C}^\times$ when v is complex infinite.

We are now ready to define the ideles.

Definition 3.1.2. Let V be the set of places of a number field K. An *idele* of K is an infinite list $(\ldots, a_v, \ldots)_{v\in V} \in \prod_{v\in V} K_v^\times$ such that $a_v \in U_v$ for all but finitely many v. The set of ideles of K is denoted J_K.

So we form an idele by making a choice of element a_v, one for each completion K_v, such that only finitely many of the a_v have absolute value different from one (with respect to the v).

The ideles were the construction of Chevalley in the 1930's in order to study class field theory in infinite extensions as well as finite ones. We will see later that the main correspondence of class field theory has a much nicer statement in terms of ideles.

The following is clear by the fact that each $K_v^\times$ is a multiplicative group with U_v as a subgroup:

Lemma 3.1.3. *The set of ideles J_K is an Abelian group under component-wise multiplication. We also have that the subset $E_K = \prod_{v\in V} U_v$ is a subgroup of J_K.*

The subgroup E_K consists of the ideles such that every entry is in the corresponding U_v. It is trivial to see that these actually are ideles.

For each place v of K we know that there is a natural inclusion $\iota_v : K \hookrightarrow K_v$ and under this inclusion we see that $\iota_v(K)$ is dense in K_v. We will just identify $\iota_v(K)$ with K where the formalities will not matter.

Since we have the above inclusions of K into K_v we can see that we have an inclusion of $K^\times$ into J_K via $\alpha \longmapsto (\ldots, \iota_v(\alpha), \ldots)$. This is the so called *diagonal embedding*. It should be noted that this really does produce an idele since every element of $K^\times$ is a unit at all but finitely many places. Again we will just refer to the image of this inclusion as $K^\times$ rather than being totally formal. When viewing $K^\times$ as the ideles above we refer to these as *principal ideles* for a reason that we shall see soon.

The group J_K is actually a locally compact topological group. To assign a topology we first note that the product topology will not work (since we have not really taken the full direct product of the $K_v^\times$'s). The topology τ we give to J_K is defined by :

$$\tau = \left\{ \prod_{v \in V} C_v \;\middle|\; C_v \text{ is an open subset of } K_v^\times \text{ for all } v \text{ and } C_v = U_v \text{ for all but finitely many } v \right\}.$$

The restriction of this topology to E_K matches the product topology we can place on E_K. To see a proof of the locally compact property see p.69 of [2].

We now have our first result in the link with ideals:

Proposition 3.1.4. *The group $J_K/K^\times E_K$ is isomorphic to the ideal class group of K.*

Proof. First we show that J_K/E_K is isomorphic to I_K, the group of fractional ideals of K.

We have a surjective homomorphism:

$$\eta : J_K \longrightarrow I_K,$$

given by :

$$(\ldots, a_v, \ldots) \longmapsto \prod_{\text{finite } v \in V} \mathfrak{p}_v^{\operatorname{ord}_v(a_v)},$$

with $\operatorname{ord}_v(a_v)$ being the $\mathfrak{p}_v$-adic valuation of $a_v \in K_{\mathfrak{p}_v}$.

Note that by the definition of the ideles, only finitely many of the a_v have $\mathfrak{p}_v$-adic absolute value different from 1. So only finitely many a_v have $\operatorname{ord}_v(a_v) \neq 0$. Thus the homomorphism always produces a finite product of prime ideals and so really maps into I_K.

Surjectivity is apparent. To see this choose any fractional ideal $\mathfrak{a}$ of K and find the prime ideal factorisation. We can choose each a_v to have order matching the corresponding power of $\mathfrak{p}_v$ in the prime ideal factorisation. This creates an idele $(\ldots, a_v, \ldots)$ that is mapped onto the original fractional ideal $\mathfrak{a}$ by η.

The kernel of this homomorphism is clearly the set of ideles with $\operatorname{ord}_v(a_v) = 0$ for all finite places v. This is the same as the set of ideles with $|a_v|_{\mathfrak{p}_v} = 1$ for all finite v and so is E_K.

Thus by the first isomorphism theorem:

$$J_K/E_K \cong I_K.$$

Next we see that for all $\alpha \in K^\times$:

$$\eta(\alpha) = \prod_{\text{finite } v \in V} \mathfrak{p}_v^{\operatorname{ord}_v(\alpha)} = \alpha \mathfrak{O}_K,$$

by realising $K^\times$ as a subgroup of J_K (so that we can apply η to elements of $K^\times$ and it is well understood).

Thus we see that:

$$J_K/K^\times E_K \cong I_K/P_K,$$

which is what we wanted. □

Now that we have seen a connection with the ideal class group can we make connections with the generalised ideal class groups?

We will spend the rest of this section forming these relationships with fractional ideals and doing things with the ideles that would be harder to do with ideals.

Definition 3.1.5. The group $C_K = J_K/K^\times$ is called the *idele class group*. This is well defined since J_K is Abelian and so $K^\times$ is automatically a normal subgroup.

The group C_K is essentially at the centre of the idele version of class field theory, and the theorems of class field theory can be rewritten in terms of this group. There is a corresponding Artin map from this group to the Galois group, and the correspondence can be rewritten in terms of certain closed subgroups of C_K.

For now we introduce the notion of modulus back into the theory. For any modulus $\mathfrak{m}$ of K we define $J_{K,\mathfrak{m}}$ to be set of ideles $(\ldots, a_v, \ldots)$ with $a_v > 0$ for all real v contained in $\mathfrak{m}$ and $a_v \equiv 1 \bmod \mathfrak{p}_v^{\mathrm{ord}_v(m)}$ for all prime ideals $\mathfrak{p}_v|\mathfrak{m}_0$. We can then define $E_{K,\mathfrak{m}}$ to be the ideles in E_K that satisfy this condition.

We now know enough to form the isomorphism with $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$. The result seems quite intuitive by the way we defined $E_{K,\mathfrak{m}}$ to match slightly the definition of $P_{K,1}(\mathfrak{m})$. This is why the proof will only be referenced.

Proposition 3.1.6. *We have that $J_K = K^\times J_{K,\mathfrak{m}}$ for any modulus $\mathfrak{m}$ of K. We also have an isomorphism:*

$$J_K/K^\times E_{K,\mathfrak{m}} \cong I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}).$$

Proof. See p.71 of [2]. □

An important corollary of this is the following:

Corollary 3.1.7. *The set of all subgroups H of J_K such that $H \supseteq K^\times E_{K,\mathfrak{m}}$ (for some modulus $\mathfrak{m}$) corresponds to the set of open subgroups of J_K that contain $K^\times$.*

Proof. See p.73 of [2]. □

Similar to ideals we can define the relative norm of ideles. Given an extension L/K of number fields the relative norm is a homomorphism:

$$N_{L/K}(.) : J_L \longrightarrow J_K.$$

I now explain how we define this.

Given any place v of K, we know by the theory of valuations that there are only finitely many extensions of v to give a place w of L. We use the notation $w|v$ to mean that w is an extension of v. So this tells us that any idele of L can have its components partitioned into finite sets, each corresponding to the places w of L such that $w|v$ for a fixed place v of K. The idea behind the norm function on the ideles is to use the corresponding completions L_w and K_v and their norm functions evaluated over these finite partitions.

Take any idele $\mathbf{a} = (\ldots, a_w, \ldots) \in J_L$. We define:

$$N_{L/K}(\mathbf{a}) = (\ldots, b_v, \ldots) \in J_K,$$

where $b_v = \prod_{w|v} N_{L_w/K_v}(a_w)$ for each place v of K.

So the v component of the idelic norm with respect to L/K is calculated by finding the finitely many places w of L such that $w|v$ and then taking the product of their corresponding norms with respect to the completions L_w and K_v. It is easy to check that the output will always be an idele since only finitely many of these completion norms will give valuations different from one.

Now that the idele norm has been defined we would hope that we can recover the last connection with the ideal version of class field theory. We hope that the group $P_{K,1}(\mathfrak{m})N_{L/K}(\mathfrak{m})$ has some kind of idele counterpart.

There is an idele version of this group but in order to get it we require the existence of a special type of modulus. We will not be able to prove any of our claims yet but for now they will be motivated. When we have some cohomology under our belt we will find that the proofs can be made.

Given an Abelian extension L/K, the group that we will find behaves most like the group $P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$ is the group $K^\times N_{L/K}(J_L)$. Again, this seems intuitive given the connections we have made with ideals so far. Unfortunately for this to be the case we are going to need the existence of a modulus $\mathfrak{m}$ such that $K^\times N_{L/K}(J_L) \supseteq E_{K,\mathfrak{m}}$.

To see why this is the case, consider the fact that $P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$ is a congruence subgroup for $\mathfrak{m}$. Indeed $N_{L/K}(\mathfrak{O}_L) = \mathfrak{O}_K$ and so $P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m})) \supseteq P_{K,1}(\mathfrak{m})$. Now by the isomorphism in Proposition 3.1.6, the idele version of congruence subgroup for a modulus $\mathfrak{m}$ of K is a subgroup H of J_K that satisfies $K^\times E_{K,\mathfrak{m}} \subseteq H \subseteq J_K$.

Clearly the group $K^\times N_{L/K}(J_L)$ contains $K^\times$ since the norm of the **1** idele of J_L is the **1** idele of J_K (the **1** idele is the idele having 1 for all of its entries). But for this group to have any hope of corresponding to $P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$ we would also have to have that $K^\times N_{L/K}(J_L)$ contains $E_{K,\mathfrak{m}}$ too for the modulus $\mathfrak{m}$, so that it is in fact a congruence subgroup for $\mathfrak{m}$ in the idelic sense (if it contains both $K^\times$ and $E_{K,\mathfrak{m}}$ then it contains $K^\times E_{K,\mathfrak{m}}$).

We do not yet know whether this group contains $E_{K,\mathfrak{m}}$ for any modulus $\mathfrak{m}$ and it is certainly not a trivial fact that there is such a modulus that makes this happen.

A consequence of the above is that we will have that:

$$[J_K : K^\times N_{L/K}(J_L)] = [I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))],$$

for all of these special moduli. It is our aim to prove these assertions.

3.2 Cohomology of finite cyclic groups

Cohomology started its life as a topological tool, roughly as a backwards version of homology. However, the theory extends to the realms of algebra. In this section we study an easy case of cohomology from first principles, the cohomology of finite cyclic groups. Once this is done we apply the theory to the ideles to get some nice results, including a proof of the claim we have just made. No prior knowledge of these topics is assumed.

In this section G will always stand for a finite cyclic group and A will stand for a G-module (an Abelian group on which G acts linearly). It is our eventual aim to take $G = \mathrm{Gal}(L/K)$ for cyclic extensions L/K and A to be either the ideles or the idele class group. For this to work we would first need to provide actions of the Galois group on these objects so that these objects really are G-modules. First we discuss the cohomology for general finite cyclic groups, applying the theory to ideles later.

Since G is a cyclic group of order $n \in \mathbb{N}$ we can choose a generator σ. We denote the identity element by 1. Now consider any G-module A and denote the fixed set of A under the action of G by A^G (these are the elements in a that are fixed by everything in G).

We note a few things:

Lemma 3.2.1. *The following things hold:*

1. *Acting as a map on A we have that $\sigma - 1$ has kernel A^G.*
2. *Acting as a map on A we have that the element $g_\sigma = 1 + \sigma + \sigma^2 + \ldots + \sigma^{n-1}$ satisfies:*
$$\mathrm{im}(g_\sigma) \subseteq A^G = \ker(\sigma - 1).$$
3. *We also have that $\mathrm{im}(\sigma - 1) \subseteq \ker(g_\sigma)$.*

Proof. This is slightly routine, remembering that the group elements act linearly on A.

For the first claim note that $\ker(\sigma - 1) = \{a \in A \,|\, (\sigma - 1)(a) = 0\} = \{a \in A \,|\, \sigma(a) = a\} = A^G$ (since if σ fixes A then so must the whole group by the cyclic nature of G).

For the second claim take some $g_\sigma(a) \in \mathrm{im}(g_\sigma)$. By the first claim it is enough to show that $g_\sigma(a)$ is in the kernel of the map $(\sigma - 1)$ on A. This is easily done since:

$$(\sigma - 1)(g_\sigma(a)) = ((\sigma - 1)(g_\sigma))(a) = ((\sigma - 1)(1 + \sigma + \ldots + \sigma^{n-1}))(a) = (\sigma^n - 1)(a) = (1 - 1)(a) = a - a = 0,$$

for all $a \in A$ (by the associative group action axiom and the fact that G acts linearly on A). Thus $g_\sigma(a) \in A^G$ proving that $\mathrm{im}(g_\sigma) \subseteq A^G$.

The third claim is similar to the second. Take $(\sigma-1)(a) \in \text{im}(\sigma-1)$ and we show that this is in the kernel of g_σ. Note that since G is cyclic it is Abelian. Thus we have that $g_\sigma(\sigma-1) = (\sigma-1)(g_\sigma) = (\sigma^n-1) = (1-1)$ as above.

Now:

$$g_\sigma((\sigma-1)(a)) = (g_\sigma(\sigma-1))(a) = (1-1)(a) = a-a = 0,$$

for all $a \in A$. Thus $(\sigma-1)(a) \in \ker(g_\sigma)$ and so $\text{im}(\sigma-1) \subseteq \ker(g_\sigma)$. □

We see that these two maps $(\sigma-1)$ and g_σ work nicely together image and kernel wise. It makes sense to define the following:

Definition 3.2.2. We define the *Herbrand quotient* of G with respect to A as:

$$Q_G(A) = \frac{[\ker(\sigma-1) : \text{im}(g_\sigma)]}{[\ker(g_\sigma) : \text{im}(\sigma-1)]} = \frac{[A^G : g_\sigma(A)]}{[\ker(g_\sigma) : (\sigma-1)(A)]},$$

whenever this value exists. Note that all kernels and images are taken to be with respect to maps on A.

The Herbrand quotient is going to be the tool we use to prove the global cyclic norm index inequality later (it is well defined by the results in Lemma 3.2.1). It satisfies a nice property for finite G-modules:

Proposition 3.2.3. *If A is a finite G-module then $Q_G(A) = 1$.*

Proof. This is really just a case of expanding the quotient and remembering that all of the things in the Herbrand quotient here are finite. We see that:

$$Q_G(A) = \frac{[\ker(\sigma-1) : \text{im}(g_\sigma)]}{[\ker(g_\sigma) : \text{im}(\sigma-1)]} = \frac{|\ker(\sigma-1)||\text{im}(\sigma-1)|}{|\ker(g_\sigma)||\text{im}(g_\sigma)|} = \frac{|A|}{|A|} = 1,$$

using the first isomorphism theorem for modules (since $\frac{|A|}{|\ker(f)|} = |\text{im}(f)|$ for any finite G-module A and any G-module homomorphism f). □

Definition 3.2.4. We define the *zeroth* and *first cohomology groups* of A with respect to G to be:

$$H^0(A) = \ker(\sigma-1)/\text{im}(g_\sigma),$$

$$H^1(A) = \ker(g_\sigma)/\text{im}(\sigma-1).$$

Note that now $Q_G(A) = \frac{|H^0(A)|}{|H^1(A)|}$ and that these cohomology groups are well defined by Lemma 3.2.1 (the quotient groups must exist by these facts).

The nice properties of the cohomology groups arise from exact sequences of G-modules. There is a useful lemma called the *exact hexagon lemma* which basically says that given an exact sequence of G-modules $0 \to A \to B \to C \to 0$ we can make an "exact hexagon" out of the corresponding zeroth and first cohomology groups (there are two such homology groups for each of A, B, C).

If the reader does not know what an exact sequence is then it does not matter since we shall never need to use this terminology again in this project. If the reader wants to see a proof of the exact hexagon lemma, then consult p.77 of [2].

The only upshot of this is that the exact hexagon lemma is used to prove the corresponding property of Herbrand quotients:

Proposition 3.2.5. *If B is a G-submodule of a G-moldule A then:*

$$Q_G(A) = Q_G(B)Q_G(A/B),$$

in such a way that whenever two of the Herbrand quotients are finite then so must be the third.

Also for any two G-modules C, D with finite Herbrand quotients we have that:

$$Q_G(C \times D) = Q_G(C)Q_G(D)$$

Proof. See p.79-p.80 of [2] for proof of the first claim. It uses the exact hexagon lemma.

For the second claim note that $C \times D$ is a G-module under the action $g(c,d) = (gc, gd)$ for all $g \in G$, $c \in C$ and $d \in D$. Take $A = C \times D$ and $B = C \times 0 \cong C$ in the first claim. Then $A/B \cong D$ and thus:

$$Q_G(C \times D) = Q_G(C)Q_G(D),$$

since it is easy to check that isomorphic G-modules have the same Herbrand quotient. □

Now we prove the following corollary:

Corollary 3.2.6. *If B is a G-submodule of a G-module A and the quotient module A/B is finite then $Q_G(A) = Q_G(B)$.*

Proof. From Proposition 3.2.3 we have that $Q_G(A/B) = 1$ since A/B is a finite G-module. Then by Proposition 3.2.5 we see that:

$$Q_G(A) = Q_G(B)Q_G(A/B) = Q_G(B).$$

□

So we can fix a group G and connect the Herbrand quotients of related G-modules. Now what happens when we change the groups too (in a related way)?

Shapiro's lemma gives us a nice connection.

Lemma 3.2.7. *(Shapiro's lemma.) Suppose that the G-module A has a subgroup decomposition:*

$$A = A_1 \oplus A_2 \oplus \ldots \oplus A_r$$

(where the A_i's are not necessarily submodules of A) and that under the action of G the A_i's are permuted transitively.

Define for each j the groups:

$$G_j = \{\tau \in G \,|\, \tau(A_j) = A_j\},$$

so that G_j is the stabilizer of each A_j under the group action. Then for each i we have that A_i is a G_i-module and $Q_G(A) = Q_{G_i}(A_i)$.

Proof. See p.80-p.82 of [2] for a (quite lengthy) proof of this. Note that each of the values $Q_{G_i}(A_i)$ makes sense since each G_i is cyclic, being a subgroup of the cyclic group G. □

We now have all of the tools we need to start work on proving the global cyclic norm index inequality. All we have to do now is to start to place a G-module structure on J_L and C_L (where L/K is some finite cyclic extension of number fields). The group G we will use will be $\mathrm{Gal}(L/K)$ which is finite and cyclic by assumption. Thus we can use all of the cohomology results for finite cyclic groups that we have above.

3.3 Galois actions on ideles

To start, take L/K to be any Galois extension of number fields. Throughout this subsection we denote $\mathrm{Gal}(L/K)$ by G for simplicity. Then G acts on the places of L via:

$$w \longmapsto \sigma w,$$

where σw is the place of L defined by:

$$|\alpha|_{\sigma w} = |\sigma^{-1}(\alpha)|$$

for all $\alpha \in L$. It is not hard to prove that this is a group action. This is left to the reader.

We define the *decomposition group* of a place w of L to be the stabilizer of w under this action. This group will be denoted G_w. Note that since finite places w of L correspond to prime ideals $\mathcal{P}_w$ of $\mathfrak{O}_L$, the decomposition group of a finite place corresponds exactly with the decomposition group $D_{\mathcal{P}_w/\mathfrak{p}_v}$ we defined earlier (where $\mathfrak{p}_v$ is just the prime ideal of $\mathfrak{O}_K$ lying under $\mathcal{P}_w$).

It should be clear by this fact that the action is transitive on all places w of L lying above a given place v of K (this is even easier to check for the extensions of infinite places).

We can also use this action to form isomorphisms between the completions K_w and $K_{\sigma w}$ for any place w of L. Denote such an isomorphism by σ too.

After this discussion we can now give J_L a G-module structure. Do this by defining (for each $\mathbf{a} = (\ldots, a_w, \ldots) \in J_L$ and $\sigma \in G$):

$$\sigma(\mathbf{a}) = (\ldots, b_w, \ldots),$$

where $b_w = \sigma(a_{\sigma^{-1}w})$.

It is quite easy to get lost in how this action works due to the abstract way it is defined. Essentially for each place v of K, this action considers the elements a_w of $\mathbf{a}$ such that the place w lies above the place v. It then permutes these a_w terms according to the action of G on the places of L. Finally, it then rewrites the result as elements of the corresponding completions via the isomorphism mentioned above (since otherwise the result would not technically be the right form for an idele; the elements have "moved" around so need to lie in the correct completions).

The way this Galois action works also allows us to make the identification of $\prod_{\sigma \in G} \sigma(\mathbf{a})$ with $N_{L/K}(\mathbf{a})$, which fits perfectly with the way norms are usually defined (as a product of Galois conjugates). This is easy to check and is left to the reader. Note that this is not an actual equality because the first idele lies in a different idele group to the second one (but if one looks at the components of both there is an obvious connection).

Note that since J_L is a G-module we can make the idele class group $C_L = J_L/L^\times$ into a G-module via $\sigma(\mathbf{a}L^\times) = \sigma(\mathbf{a})L^\times$ for all $\sigma \in G$ and $\mathbf{a} \in J_L$. Thus there is a similar notion of norm on C_L (giving classes of C_K as its output).

We are hoping to use the Herbrand quotient on these two G-modules, but before we can do this we need to be able to find out what J_L^G and C_L^G are. We get a nice result when we work these things out.

Theorem 3.3.1. *We have that:*

$$J_L^G \cong J_K$$
$$C_L^G \cong C_K.$$

Proof. We prove the first isomorphism. The second follows from the first (with a slight use of Hilbert's theorem 90). See p.85-p.86 of [2] for the proof of this.

Take $\mathbf{a} \in J_L^G$ so that $\sigma(\mathbf{a}) = \mathbf{a}$ for all $\sigma \in G$. Also fix a place v of K. Then $a_w = \sigma(a_{\sigma^{-1}w})$ for all $\sigma \in G$ and all places w of L with $w|v$ (this is just the rule of the action along with the fact that $\mathbf{a}$ is fixed by all σ).

Now this equality is certainly satisfied by the decomposition group since it is satisfied for all elements of the Galois group. Taking only those $\sigma \in G_w$ we see that $a_w = \sigma(a_w)$ for all such $w|v$.

It can be checked that the decomposition group of a given w with $w|v$ is the same as the Galois group of the extension of completions L_w/K_v. Thus, by basic Galois theory along with the fact that $a_w = \sigma(a_w)$ for each $w|v$, we see that actually $a_w \in K_v$ for all such w (since by the Galois correspondence K_v is the fixed field corresponding to the whole decomposition group).

It remains to check that actually all of the a_w terms corresponding to the fixed place v are equal. Suppose that w_1 and w_2 are two places lying above v. We show that $a_{w_1} = a_{w_2}$.

By the transitivity of the Galois action mentioned above, there must exist $\tau \in$ G such that $\tau w_1 = w_2$. But then $w_1 = \tau^{-1} w_2$ and so it follows that $a_{w_2} = \tau(a_{w_1})$ (since we had above that $a_w = \sigma(a_{\sigma^{-1}w})$ for all $\sigma \in G$). Since both a_{w_1} and a_{w_2} lie in K_v it must be that $a_{w_1} = a_{w_2}$.

Now we are done since we now know that the v component of any element of J_L^G is of the form $(b_v, b_v, \ldots, b_v)$ with $b_v \in K_v$. There is a clear isomorphism with J_K here by just taking one b_v from each grouping, i.e.:

$$(\ldots, (b_v, b_v, \ldots, b_v), \ldots) \longmapsto (\ldots, b_v, \ldots) \in J_K.$$

□

We end by getting halfway to proving the global cyclic norm index inequality.

Theorem 3.3.2. *Let L/K be a cyclic extension with Galois group generated by σ. We have that (with respect to the action on C_L):*

$$[C_L^G : \mathrm{im}(g_\sigma)] = [J_K : K^\times N_{L/K}(J_L)].$$

Proof. Here we find that:

$$\mathrm{im}(g_\sigma) = N_{L/K}(C_L),$$

where the norm of an idele class $\mathbf{a}L^\times \in C_L$ is defined by:

$$N_{L/K}(\mathbf{a}L^\times) = N_{L/K}(\mathbf{a})K^\times \in C_K.$$

Also we know that $C_L^G \cong C_K$ so that $[C_L^G : \mathrm{im}(g_\sigma)] = [C_K : N_{L/K}(C_L)]$.

It is clear that:

$$N_{L/K}(C_L) \cong N_{L/K}(J_L)/(K^\times \cap N_{L/K}(J_L)).$$

.

Using the 2nd isomorphism theorem we now see that:

$$N_{L/K}(J_L)/(K^\times \cap N_{L/K}(J_L)) \cong (K^\times N_{L/K}(J_L))/K^\times.$$

But then:

$$[C_K : N_{L/K}(C_L)] = [J_K/K^\times : (K^\times N_{L/K}(J_L))/K^\times] = [J_K : K^\times N_{L/K}(J_L)].$$

□

The importance of this result will be made clear later when we make an explicit calculation of the Herbrand quotient of C_L (for cyclic extensions L/K).

4 Proving the main results

Now that we have seen how the ideles connect with the ideal version of class field theory we can get down to proving the results. We have nearly all of the tools we willl need. Let K be a number field as usual.

Firstly we pause to prove that all generalized ideal classes are finite for any modulus $\mathfrak{m}$ of K.

Theorem 4.0.3. *Let K be a number field and $\mathfrak{m}$ be a modulus of K. Then all generalised ideal class groups for $\mathfrak{m}$ are finite.*

Proof. We show that the group $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$ is finite and then by the inclusion $P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m})$, it must follow that all generalised ideal class groups are finite (recall that all generalised ideal class groups are of the form $I_K(\mathfrak{m})/H$ for some group H as described above).

Recall that the ideal class group I_K/P_K is a finite group (this was remarked on in the previous project). The result we seek is going to follow from a chain of homomorphisms and isomorphisms.

First we establish the isomorphism:

$$I_K(\mathfrak{m})/P_K(\mathfrak{m}) \cong I_K/P_K$$

To see this we show that every class of ideals in I_K/P_K contains an ideal coprime to $\mathfrak{m}$. Take a fractional ideal $\mathfrak{a}$ that lies in a given class of the ideal class group.

If $\mathfrak{a}$ is coprime to $\mathfrak{m}$ then we are done. If not then for each $\mathfrak{p}|\mathfrak{m}_0$ we let $r_\mathfrak{p}$ denote the highest power of $\mathfrak{p}$ that divides $\mathfrak{a}$. Choose elements $\pi_\mathfrak{p}$ for each $\mathfrak{p}$ such that $\pi_\mathfrak{p} \in \mathfrak{p}$ but $\pi_\mathfrak{p} \notin \mathfrak{p}^2$ (this is equivalent to the ideal $(\pi_\mathfrak{p})$ being divisible by $\mathfrak{p}$ but not by $\mathfrak{p}^2$).

By the Chinese remainder theorem there is a unique solution $\alpha \in \mathfrak{O}_K$ to the congruences:

$$\alpha \equiv \pi_\mathfrak{p}^{r_\mathfrak{p}} \bmod \mathfrak{p}^{r_\mathfrak{p}+1}$$

Now consider the fractional ideal $\mathfrak{a}(\alpha^{-1})$. This lies in the same class of I_K/P_K as $\mathfrak{a}$ since it is a principal fractional ideal multiple of $\mathfrak{a}$. Also $\mathfrak{a}(\alpha^{-1})$ is not divisible by any $\mathfrak{p}|\mathfrak{m}_0$ and so it is coprime to $\mathfrak{m}$.

Thus we have a surjective homomorphism:

$$I_K(\mathfrak{m}) \longrightarrow I_K/P_K$$

$$\mathfrak{a} \longmapsto \mathfrak{a}P_K$$

with kernel $P_K \cap I_K(\mathfrak{m}) = P_K(\mathfrak{m})$, giving the isomorphism:

$$I_K(\mathfrak{m})/P_K(\mathfrak{m}) \cong I_K/P_K$$

Now we use the fact that:

$$P_{K,1}(\mathfrak{m}) \subset P_K(\mathfrak{m}) \subset I_K(\mathfrak{m})$$

to see that there exists (by inclusion) a surjective homomorphism:

$$I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) \longrightarrow I_K(\mathfrak{m})/P_K(\mathfrak{m})$$

$$\mathfrak{a}P_{K,1}(\mathfrak{m}) \longmapsto \mathfrak{a}P_K(\mathfrak{m})$$

the kernel being $P_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$.

Now we relate this to elements of $K^\times$. We can form two subgroups of $K^\times$. Firstly, we have the subgroup $K(\mathfrak{m})$ consisting of the elements $\alpha \in K^\times$ such that the fractional ideal (α) is coprime to $\mathfrak{m}$. Secondly, we have the subgroup $K_1(\mathfrak{m})$ consisting of the elements $\alpha \in K^\times$ such that $\alpha \equiv 1 \bmod \mathfrak{m}_0$ and $\sigma(\alpha) > 0$ for all real embeddings of K lying in $\mathfrak{m}_\infty$. Denote the unit group $\mathfrak{O}_K^\times$ as U_K.

It should now be of no surprise that the map:

$$K(\mathfrak{m}) \longrightarrow P_K(\mathfrak{m})$$

$$\alpha \longmapsto (\alpha)$$

is a surjective homomorphism too and that we can make from this the isomorphism:

$$K(\mathfrak{m})/U_K K_1(\mathfrak{m}) \cong P_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$$

since the inverse image of $P_{K,1}(\mathfrak{m})$ under the homomorphism is exactly $U_K K_1(\mathfrak{m})$ (associates generate the same ideal).

It remains to show that $K(\mathfrak{m})/U_K K_1(\mathfrak{m})$ is a finite group. Note that since $1 \in U_K$ we have that:

$$K(\mathfrak{m}) \supseteq U_K K_1(\mathfrak{m}) \supseteq K_1(\mathfrak{m}),$$

thus it suffices to prove that $K(\mathfrak{m})/K_1(\mathfrak{m})$ is finite.

We form a homomorphism:

$$K(\mathfrak{m}) \longrightarrow (\mathfrak{O}_K/\mathfrak{m})^\times \times \{1,-1\}^r,$$

where r is the number of real embeddings of K.

This map sends $\alpha \in K(\mathfrak{m})$ to $(\beta\gamma^{-1}+\mathfrak{m})(\text{sign}(\sigma_1(\alpha)), \text{sign}(\sigma_2(\alpha)), \ldots, \text{sign}(\sigma_r(\alpha)))$, where $\beta, \gamma \in \mathfrak{O}_K$ are such that $\alpha = \frac{\beta}{\gamma}$ and $\sigma_1, \sigma_2, \ldots, \sigma_r$ are the real embeddings of K (recall that K is the field of fractions of $\mathfrak{O}_K$ so such β, γ exist). It can be shown that this is a surjection with kernel $K_1(\mathfrak{m})$.

Thus $K(\mathfrak{m})/K_1(\mathfrak{m}) \cong (\mathfrak{O}_K/\mathfrak{m})^\times \times \{1,-1\}^r$ and the group on the right has a finite order (it has $2^r N(\mathfrak{m})$ elements). □

4.1 The universal norm index inequality

In this subsection we prove the first of the two inequalities that will be useful later. In order to tackle the proof we require specific L-series constructed from the characters of the finite group $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$ (where L/K is an Abelian extension of number fields and $\mathfrak{m}$ is a complete modulus for L/K).

No preliminary knowledge of L-series is needed although I shall only motivate the results here. The material is not directly important to this project but an interested reader can consult Chapter VIII of [1] for proofs and discussions that are omitted.

Recall that given a sequence $\{a_n\}$ of complex numbers we can define the corresponding *Dirichlet series*:

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where s is a complex variable.

The convergence of Dirichlet series falls into one of three scenarios:

1. The series converges for all $s \in \mathbb{C}$.
2. The series diverges for all $s \in \mathbb{C}$.
3. There exists a complex number s_0 such that $L(s)$ converges for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > \mathrm{Re}(s_0)$ and diverges for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) < \mathrm{Re}(s_0)$ (in which case we call $\mathrm{Re}(s_0)$ the *abscissa of convergence*, a notion analogous to the radius of convergence in power series).

Also, more can be said about the convergence when the a_n behave in a nice way:

- If the a_n are bounded (i.e. all have complex modulus less than some fixed real number) then immediately we can say that $L(s)$ converges absolutely for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$.
- If the partial sums $A_n = a_1 + a_2 + \ldots a_n$ are bounded for all n then immediately we can say that $L(s)$ converges for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 0$.
- If $L(s)$ converges at some s_0 then $L(s)$ converges absolutely for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > \mathrm{Re}(s_0) + 1$.

A special Dirichlet series in number theory is the *Riemann zeta function*. To start with, this is the Dirichlet series obtained by using the sequence $a_n = 1$ for all n:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

It is clear that this series does not converge for $s = 1$ (we get the harmonic series, which is divergent) but by a comparison test we find that $\zeta(s)$ converges for all real $s > 1$. This fact combined with the above discussion tells us that $\zeta(s)$ converges for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ (and diverges in the half plane $\mathrm{Re}(s) < 1$).

With use of the Dirichlet series:

$$\zeta_2(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s} = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \ldots,$$

(which by the above is convergent for all complex s with $\mathrm{Re}(s) > 0$) we can extend the definition of $\zeta(s)$ to account for the "bigger" half plane $\mathrm{Re}(s) > 0$.

To see how this works consider:

$$\zeta(s) - \zeta_2(s) = 2\sum_{k=1}^{\infty} \frac{1}{(2k)^s} = \frac{1}{2^{s-1}} \sum_{k=1}^{\infty} \frac{1}{k^s} = \frac{1}{2^{s-1}}\zeta(s),$$

giving:

$$\zeta(s) = \frac{\zeta_2(s)}{1 - \frac{1}{2^{s-1}}}.$$

This extended version of the Riemann zeta function is clearly analytic everywhere in the half plane $\mathrm{Re}(s) > 0$ except for a simple pole at $s = 1$ (with residue 1). These facts follow by the convergence properties of $\zeta_2(s)$ and the extra $1 - \frac{1}{2^{s-1}}$ factor.

Actually, the Riemann zeta function can be extended further to give a function analytic on the whole complex plane except for the above mentioned simple pole. This was a little of what Riemann himself achieved in his famous 1859 paper (see [5]) using a complicated functional equation. It is also this paper that contains the first ever mention of the Riemann hypothesis. We will not need the full Riemann zeta function so nothing more will be said about it.

By unique factorisation into primes in $\mathbb{Z}$, we can find the *Euler product*:

$$\zeta(s) = \prod_{\text{primes } p} \frac{1}{1 - \frac{1}{p^s}},$$

valid for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. This forms an interesting relationship between prime numbers and the Riemann zeta function.

Taking logs of this relationship (which is possible, take this on trust) and expanding using Taylor series we see that:

$$\ln(\zeta(s)) = \sum_p \sum_m \frac{1}{mp^{ms}},$$

where m runs through the positive integers and p runs through the prime numbers. Taking all of the terms with $m \geq 2$ in the above sum gives a sum that is absolutely convergent at $s = 1$. We find that only the sum:

$$\sum_p \frac{1}{p^s}$$

can possibly contribute to the simple pole of the zeta function at $s = 1$.

Given two complex functions f and g, both having singularities at 1, we use the notation $f(x) \sim g(x)$ to mean that the function $f(x) - g(x)$ is analytic at 1. This measures the asymptotic behaviour at $s = 1$. It can be shown by an integral comparison (with $\int_1^\infty \frac{1}{x^s}\, dx$) that:

$$\zeta(s) \quad \sim \quad \frac{1}{s-1}$$

and so it follows by the above facts that:

$$\ln(\zeta(s)) \quad \sim \quad \sum_p \frac{1}{p^s} \quad \sim \quad \ln\left(\frac{1}{s-1}\right).$$

The reason we have gone into so much detail with the Riemann zeta function is because there is a generalisation to all number fields. The Riemann zeta function can be thought of as a sum over the norms of ideals of the ring of integers $\mathbb{Z}$ of the number field $\mathbb{Q}$.

Definition 4.1.1. We define for a general number field K the *Dedekind zeta function* $\zeta_K(s)$, defined by:

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

where $\mathfrak{a}$ runs through all non-zero ideals of $\mathfrak{O}_K$.

As a generalisation, the Dedekind zeta function is also absolutely convergent for all complex s in the half plane $\mathrm{Re}(s) > 1$. Also in the same way as the Riemann zeta function we can use unique factorisation into prime ideals in $\mathfrak{O}_K$ to get an Euler product:

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}$$

where $\mathfrak{p}$ runs through the prime ideals of $\mathfrak{O}_K$.

In terms of asymptotics around $s = 1$ it can be shown that:

$$\ln(\zeta_K(s)) = \sum_{\mathfrak{p}} \sum_{m} \frac{1}{m(N(\mathfrak{p}))^{ms}} \quad \sim \quad \sum_{\deg(\mathfrak{p})=1} \frac{1}{N(\mathfrak{p})^s},$$

where $\deg(\mathfrak{p}) = 1$ stands for all prime ideals of $\mathfrak{O}_K$ that have a prime number norm. These results also agree with the earlier work.

But we can go even further. We can partition the terms in the sum of $\zeta_K(s)$ since every ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ lies in one of the finitely many classes of the ideal class group I_K/P_K. Let $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_{h_K}$ represent the classes of I_K/P_K.

Using this we may write:

$$\zeta_K(s) = \sum_{i=1}^{h_K} \zeta(s, \mathcal{A}_i),$$

where:

$$\zeta(s, \mathcal{A}_i) = \sum_{\mathfrak{a} \in \mathcal{A}_i} \frac{1}{(N(\mathfrak{a}))^s}.$$

Each $\zeta_K(s, \mathcal{A}_i)$ can be shown to be analytic for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$, except for a simple pole at $s = 1$ as usual. Studying the Dedekind zeta function in this form and the residue of this simple pole leads to nice results on the class number h_K but we shall not concern ourselves with this here.

Generalizing further we can take any modulus $\mathfrak{m}$ of K and form the similar sum:

$$\zeta_K(s, \mathfrak{m}) = \sum_{\mathfrak{a}, \mathfrak{m}_0 \text{ coprime}} \frac{1}{(N(\mathfrak{a}))^s}.$$

We can give this the Euler product:

$$\zeta_K(s, \mathfrak{m}) = \prod_{\mathfrak{p} \nmid \mathfrak{m}_0} \frac{1}{1 - \frac{1}{(N(\mathfrak{p}))^s}},$$

the product being roughly the same as the Euler product for $\zeta_K(s)$ but missing only finitely many terms (the ones that correspond to the finitely many prime ideals that divide $\mathfrak{m}_0$).

If we let $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_t$ be a set of representatives for the classes of $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$ then we can see that:

$$\zeta_K(s, \mathfrak{m}) = \sum_{i}^{t} \zeta_K(s, \mathcal{B}_i),$$

where:

$$\zeta_K(s, \mathcal{B}_i) = \sum_{\mathfrak{a} \in \mathcal{B}_i} \frac{1}{(N(\mathfrak{a}))^s}.$$

As earlier each $\zeta_K(s, \mathfrak{b}_i P_{K,1}(\mathfrak{m}))$ can be shown to be analytic for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$, except for the usual simple pole at $s = 1$. Studying the residue of the simple pole this time relates to the order of the generalised ideal class group $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$. This should strike the reader as a very interesting conclusion,

that the residue of the simple pole each time seems to be giving lots of important information on class numbers and related things.

Before defining the corresponding L-series we note the following asymptotic behaviour:

$$\ln(\zeta_K(s)) \quad \sim \quad \ln\left(\frac{1}{s-1}\right) \quad \sim \quad \sum_{\mathfrak{p}} \frac{1}{(N(\mathfrak{p}))^s} \quad \sim \quad \sum_{\deg(\mathfrak{p})=1} \frac{1}{(N(\mathfrak{p}))^s}.$$

We are now close to a proof of the universal norm index inequality. In order to prove it we need to use L-series. These types of series were first used by Dirchlet in order to prove his theorem on the infinitude of primes in arithmetic progressions.

Recall that a character of a group G is a group homomorphism $\chi : G \longrightarrow \mathbb{C}^\times$. Given two characters χ, ψ of a group G we define the product $\chi\psi$ to be the character defined by $(\chi\psi)(g) = \chi(g)\psi(g)$ for all $g \in G$. The characters of a group then form a group under this multiplication, the *character group* of G, denoted $\hat{G}$. The identity element of this group is the trivial character χ_0 that satisfies $\chi_0(g) = 1$ for all $g \in G$. When G is a finite Abelian group we have that $G \cong \hat{G}$.

We have the following:

Lemma 4.1.2. *Let G be a finite Abelian group and $\chi \in \hat{G}$. Then:*

$$\sum_{g\in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise} \end{cases}$$

Proof. When χ is trivial then it is clear that the sum is the same as $|G|$ since $\chi(g) = 1$ for all $g \in G$.

Suppose χ is non trivial. Then there exists some $h \in G$ with $\chi(h) \neq 1$. By basic group theory, as g runs through the elements of G so does hg.

Thus:

$$\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(hg) = \chi(h) \sum_{g\in G} \chi(g),$$

from which it follows that $(\chi(h) - 1)(\sum_{g\in G} \chi(g)) = 0$. But $\chi(h) \neq 1$, thus $\sum_{g\in G} \chi(g) = 0$. □

There is a similar result if we fix some $g \in G$ and sum over all characters. We get $|G|$ if g is the identity element and 0 otherwise. Also as mentioned in [1] we can extend results like this to the infinite case. When we have a compact Abelian group we can place the Haar measure on it and consider certain integrals similar to the sum above. These integrals show nice results.

Now we are able to make an L-series. Essentially the examples of Dirichlet series we have had so far all corresponded to having 1 on the numerator of every term. But this can be realised as just being the trivial character of each element in the group under consideration. If we use different characters instead we get a more general type of series.

The L-series that Dirichlet constructed in his proof of the infinitude of primes in arithmetic progressions were of the form:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

where χ is a specific mod n Dirichlet character (basically a character of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ but defined to be able to take any integer input rather than a class of integers). The proof basically boils down to considering the finitely many series of this form, one for each character, and finding the right linear combination to produce something that is directly related to a given class of integers mod n. Then the divergence of this new series guarantees that there must be infinitely many primes in that given class.

We now use the series $\zeta_K(s, \mathfrak{m})$ defined above to construct L-series in a similar way.

Definition 4.1.3. Let $\mathfrak{m}$ be a modulus of a number field K and let χ be a character of the finite group $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$, defined on $I_K(\mathfrak{m})$ by $\chi(\mathfrak{a}) = \chi(\mathfrak{a}P_{K,1}(\mathfrak{m}))$ (i.e. applying χ to $\mathfrak{a} \in I_K(\mathfrak{m})$ gives the same as applying χ to the class $\mathfrak{a}P_{K,1}(\mathfrak{m})$).

We define the L-series $L_K(s, \mathfrak{m}, \chi)$ as follows:

$$L_K(s, \mathfrak{m}, \chi) = \sum_{\mathfrak{a}, \mathfrak{m} \text{ coprime}} \frac{\chi(\mathfrak{a})}{(N(\mathfrak{a}))^s}.$$

These L-series should just be thought of as generalisations of the Dedekind zeta functions we had earlier, except now the numerators are allowed to take other values (but values that still have a nicely behaved multiplicative structure to them).

As usual we have an Euler product:

$$L_K(s, \mathfrak{m}, \chi) = \prod_{\mathfrak{p} \nmid \mathfrak{m}_0} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{(N(\mathfrak{p}))^s}}.$$

Also when taking logs we get a similar result to earlier:

$$\ln(L_K(s, \mathfrak{m}, \chi)) = \sum_{m, \mathfrak{p} \nmid \mathfrak{m}_0} \frac{(\chi(\mathfrak{p}))^m}{m(N(\mathfrak{p}))^{ms}},$$

valid for all $s \in \mathbb{C}$ such that $\text{Re}(s) > 1$. Using this we get the usual asymptotic relation:

$$\ln(L_K(s, \mathfrak{m}, \chi)) \quad \sim \quad \sum_{\mathfrak{p} \nmid \mathfrak{m}_0, \deg(\mathfrak{p}) = 1} \frac{\chi(\mathfrak{p})}{(N(\mathfrak{p}))^s}.$$

Finally we can use the partitioning trick from earlier to write:

$$L_K(s, \mathfrak{m}, \chi) = \sum_i \chi(\mathcal{A}_{i,\mathfrak{m}}) \zeta_K(s, \mathcal{A}_{i,\mathfrak{m}}),$$

where $\mathcal{A}_{1,\mathfrak{m}}, \mathcal{A}_{2,\mathfrak{m}}, \ldots, \mathcal{A}_{t,\mathfrak{m}}$ are representatives for the classes of $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$.

The convergence of $L_K(s, \mathfrak{m}, \chi)$ when χ is non-trivial is nicer than when χ is trivial. When χ is non-trivial we have convergence for all $s \in \mathbb{C}$ with $\text{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$ and so in this case there is no pole at $s = 1$. When χ is trivial we already know from earlier that there is a simple pole at $s = 1$.

We are now ready to prove the universal norm index inequality.

Theorem 4.1.4. *(Universal norm index inequality) Let L/K be an Abelian extension of number fields and let $\mathfrak{m}$ be a modulus of K. Then we have the inequality:*

$$[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m}) N_{L/K}(I_L(\mathfrak{m}))] \leq [L : K].$$

Proof. Let $H = P_{K,1}(\mathfrak{m}) N_{L/K}(I_L(\mathfrak{m}))$, $h = [I_K(\mathfrak{m}) : H]$ and let χ be a non-trivial character of $I_K(\mathfrak{m})/H$. By the inclusion of $P_{K,1}(\mathfrak{m})$ in H, we can view χ as a character of $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$.

Since $L_K(s, \mathfrak{m}, \chi)$ has no pole at $s = 1$ we can write:

$$L_K(s, \mathfrak{m}, \chi) = (s-1)^{m(\chi)} g(s, \chi),$$

for some $m(\chi) \geq 0$ (where the function g has neither a zero nor a pole at $s = 1$). This is just the pulling out the root $s = 1$ of multiplicity $m(\chi)$. It will actually follow soon that $m(\chi) = 0$.

Let $\mathcal{A}_{1,\mathfrak{m}}, \mathcal{A}_{2,\mathfrak{m}}, \ldots, \mathcal{A}_{h,\mathfrak{m}}$ be the classes of the quotient group $I_K(\mathfrak{m})/H$. Taking logs we see that:

$$\ln(L_K(s, \mathfrak{m}, \chi)) \quad \sim \quad m(\chi) \ln(s-1) = -m(\chi) \ln\left(\frac{1}{s-1}\right).$$

Also we know that for $\text{Re}(s) > 1$:

$$\ln(L_K(s, \mathfrak{m}, \chi)) \quad \sim \quad \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{(N(\mathfrak{p}))^s} = \sum_{i=1}^{h} \chi(\mathcal{A}_{i,\mathfrak{m}}) \sum_{\mathfrak{p} \in \mathcal{A}_{i,\mathfrak{m}}} \frac{1}{(N(\mathfrak{p}))^s}.$$

This comes by partitioning the prime ideals into their respective classes of $I_K(\mathfrak{m})/H$ and noting that by definition the character of a prime ideal and its corresponding class are equal.

Summing over all characters of $I_K(\mathfrak{m})/H$ we see that:

$$\ln(\zeta_K(s,\mathfrak{m})) + \sum_{\chi\neq\chi_0} \ln(L_K(s,\mathfrak{m},\chi)) \quad \sim \quad \sum_{\chi}\sum_{i=1}^{h}\left(\chi(\mathcal{A}_{i,\mathfrak{m}}) \sum_{\mathfrak{p}\in\mathcal{A}_{i,\mathfrak{m}}} \frac{1}{(N(\mathfrak{p}))^s}\right),$$

since for the trivial character χ_0 we have $L_K(s,\mathfrak{m},\chi_0) = \zeta_K(s,\mathfrak{m})$.

But we know that (for all $\chi \neq \chi_0$):

$$\ln(\zeta_K(s,\mathfrak{m})) \quad \sim \quad \ln\left(\frac{1}{s-1}\right)$$

$$\ln(L_K(s,\mathfrak{m},\chi)) \quad \sim \quad -m(\chi)\ln\left(\frac{1}{s-1}\right).$$

Now take s to be a real variable with $s > 1$. We must have that (by considering what happens as $s \to 1$ from the right):

$$\left[1 - \sum_{\chi\neq\chi_0} m(\chi)\right] \ln\left(\frac{1}{s-1}\right) \quad \sim \quad h\sum_{\mathfrak{p}\in H} \frac{1}{(N(\mathfrak{p}))^s}.$$

This is because both sides have a simple pole at $s = 1$ with the same residue, so the difference of the two functions must be analytic at $s = 1$ as well as everywhere else.

Consider the set $S_{L/K}$ consisting of all prime ideals of $\mathfrak{O}_K$ that split completely in L. Thus for each $\mathfrak{p} \in S_{L/K}$ we have exactly $[L : K]$ primes $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_{[L:K]}$ of $\mathfrak{O}_L$ lying above $\mathfrak{p}$. Note that here it follows that $N(\mathcal{P}_i) = N(\mathfrak{p})$ for all i (using towers of norms, $N_{L/\mathbb{Q}}(\mathcal{P}_i) = N_{K/\mathbb{Q}}(N_{L/K}(\mathcal{P}_i)) = N_{K/\mathbb{Q}}(\mathfrak{p})$ so that $N(\mathcal{P}_i) = N(\mathfrak{p})$).

Note also that by the above each prime that splits completely in L lies in H (since it is a norm of a fractional ideal prime to $\mathfrak{m}\mathfrak{O}_L$ in L) and so we have that:

$$h\sum_{\mathfrak{p}\in H} \frac{1}{(N(\mathfrak{p}))^s} \quad \succeq \quad h\sum_{\mathfrak{p}\in S_{L/K}} \frac{1}{(N(\mathfrak{p}))^s},$$

where $f(x) \succeq g(x)$ means that f is greater than g upto a constant in a neighbourhood of 1.

But we now have that:

$$h\sum_{\mathfrak{p}\in S_{L/K}} \frac{1}{(N(\mathfrak{p}))^s} \quad \succeq \quad \frac{h}{[L:K]}\sum_{\deg(\mathcal{P})=1} \frac{1}{(N(\mathcal{P}))^s} \quad \sim \quad \frac{h}{[L:K]}\ln\left(\frac{1}{s-1}\right),$$

taking the $\mathcal{P}$ to be prime ideals of $\mathfrak{O}_L$.

It now follows that:

$$\left[1 - \sum_{\chi\neq\chi_0} m(\chi)\right] \ln\left(\frac{1}{s-1}\right) \quad \succeq \quad \frac{h}{[L:K]}\ln\left(\frac{1}{s-1}\right),$$

from which it follows that $m(\chi) = 0$ for all non-trivial χ (recall that the $m(\chi)$ are non-negative integers and that $\frac{h}{[L:K]} > 0$). Finally we find that $h \leq [L : K]$, which is what we wanted to prove. □

4.2 The global cyclic norm index inequality

We have just seen the inequality $[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))] \leq [L : K]$ for any Abelian extension L/K and any modulus $\mathfrak{m}$ for L/K. The next step is to try and turn this into an equality. If we can show the reverse inequality $[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))] \geq [L : K]$ then we will be done. Unfortunately this inequality is

not always true, it requires a special modulus (remarked upon at the end of Section 3.1). Also we find that this particular inequality is easier to prove for cyclic extensions (even though it will become true for Abelian extensions after we prove the main theorems of class field theory).

Our strategy in proving this inequality will first be to show that there are special moduli $\mathfrak{m}$ such that $[J_K : K^\times N_{L/K}(J_L)] = [I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))]$. This then allows us to move into the realm of ideles and use the cohomology results we found in Section 3.3. Finally we will calculate the Herbrand quotient of C_L explicitly and then after relating the answer with Theorem 3.3.2, the inequality will come as a corollary.

Most of the results in this section will actually be true for Abelian extensions but since we have only used the cohomology of cyclic groups we must retreat to proving things for cyclic extensions only. Again we denote $\mathrm{Gal}(L/K)$ by G in this subsection for simplicity.

To make a start on this process we first need to consider how the Herbrand quotient works around extensions of local fields (i.e. field extensions of completions).

Fix a place v of K and consider for places w of L:

$$U_{v,L} = \prod_{w|v} U_w,$$

where the U_w are the unit groups defined in Definition 3.1.1. By restriction of the action of G on J_L we see that $U_{v,L}$ is a G-module for each v (we are permuting things with absolute value 1).

By Shapiro's lemma we have that $Q_G(U_{v,L}) = Q_{G_w}(U_w)$ for each $w|v$, where G_w is the decomposition group defined earlier. Since each G_w is isomorphic to the group $\mathrm{Gal}(L_w/K_v)$ we see that each U_w is a $\mathrm{Gal}(L_w/K_v)$-module. We study the values of $Q_{\mathrm{Gal}(L_w/K_v)}(U_w)$ when we work in cyclic extensions of local fields.

Lemma 4.2.1. *Let L_w/K_v be a cyclic extension of local fields. Then $Q_{\mathrm{Gal}(L_w/K_v)}(U_w) = 1$ and:*

$$[U_w^{\mathrm{Gal}(L_w/K_v)} : \mathrm{im}(g_\sigma)] = [U_v : N_{L_w/K_v}(U_w)] = e,$$

where e is the ramification index of the Galois extension L_w/K_v.

In Abelian extensions of local fields we instead get the inequality $[U_v : N_{L_w/K_v}(U_w)] \leq e$.

Proof. See p.88-p.91 of [2]. The proof is too long to include here and relies heavily on Hilbert's Theorem 90, along with p-adic power series. □

Now we are able to prove the existence of the special moduli mentioned earlier.

Corollary 4.2.2. *Let L/K be an Abelian extension of number fields. Then there exists a modulus $\mathfrak{m}$ of K such that $H = K^\times N_{L/K}(J_L) \supseteq E_{K,\mathfrak{m}}$ (and H is open in J_K). Further, for all such moduli we have the the equality $[J_K : K^\times N_{L/K}(J_L)] = [I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))]$.*

Proof. We shall prove only the first claim. The second is not as trivial as it seems but can be found on p.92 of [2].

We first note the inclusions:

$$H \supseteq N_{L/K}(J_L) \supseteq N_{L/K}(E_L) = \prod_v \prod_{w|v} N_{L_w/F_v}(U_w).$$

Consider first the case where v is a finite place. For the places w lying above v that are unramified we have that $e = 1$ in the above result and so $[U_v : N_{L_w/K_v}(U_w)] = 1$ leading to the equality $N_{L_w/K_v}(U_w) = U_v$. As an aside, this is a strong result telling us that the local norm is surjective for finite places that are unramified. So the group $N_{L_w/K_v}(U_w)$ is open here.

For the places w lying above v that are ramified (with exponent e) we have that $[U_v : N_{L_w/K_v}(U_w)] \leq e$. By the continuity of the local norm maps $N_{L_w/K_v}(.)$, we must have that $N_{L_w/K_v}(U_w)$ is compact. This tells us that $N_{L_w/K_v}(U_w)$ here is a closed subgroup of finite index in U_v (which is a compact group). But we know that U_v is a topological group and it is a general result in such groups that closed subgroups of finite index are also open. Using this result it follows that $N_{L_w/K_v}(U_w)$ must also be open in the ramified case.

Next consider the case where v is an infinite place. Here U_w can take one of two forms, $\mathbb{C}^\times$ or $\mathbb{R}^\times$, so that $N_{L_w/K_v}(U_w)$ can only take one of three forms, $\mathbb{C}^\times, \mathbb{R}^\times$ or $\mathbb{R}^\times_+$ (the positive non-zero real numbers). All of these are open too.

But E_K has the product topology, so $N_{L/K}(E_L)$ must be open in E_K. Then it follows by the theory of topological groups and the inclusions above that H is open in J_K.

Since H is open and clearly contains $K^\times$, it follows by Corollary 3.1.7 that there is some modulus $\mathfrak{m}$ such that $H \supseteq E_{K,\mathfrak{m}}$. □

Actually it can be shown that there exists a modulus $\mathfrak{m}$ satisfying the above that is divisible only by ramified primes of L/K. To see this consider an open neighbourhood A of the idele $\mathbf{1}$ in H (this exists since we have just shown H to be open). We can write $A = \prod_v A_v$ where $A_v = U_v$ for all but finitely many places v and:

$$A_v = \begin{cases} 1 + \mathfrak{p}_v^{n_v} & \text{if } v \text{ is finite} \\ \{x \in K_v \mid |x-1|_v \leq \epsilon\} & \text{if } v \text{ is infinite} \end{cases}$$

for the other places (each n_v is a positive integer and $\epsilon > 0$ is a real number). Take our modulus $\mathfrak{m}$ to consist of the places that fall into the second category (i.e. the ones where $A_v \neq U_v$).

It is clear by surjectivity of local norms at unramified places that we can now provide a neighbourhood of $\mathbf{1}$ in H for which $A_v = U_v$ at all unramified places. This modulus $\mathfrak{m}$ will still satisfy $H \supseteq E_{K,\mathfrak{m}}$ and will only be divisibly by ramified primes, as required. This is because in topological groups we only need to find an open neighbourhood of the identity element to be able to claim that a given subgroup is open.

At the moment this does not imply that this $\mathfrak{m}$ is divisible by *all* ramified primes in L/K, just that the only prime divisors of $\mathfrak{m}$ are ramified ones in L/K. This property follows from the proof above. Later, when we have proved the main theorems of class field theory, it will follow that such a modulus must be divisible by all of the ramified primes.

It can also be shown that there is a minimal modulus $\mathfrak{f}$ such that $K^\times N_{L/K}(J_L) \supseteq E_{K,\mathfrak{f}}$ (minimal in the sense of divisibility of moduli). This modulus is called the *conductor* of the extension L/K.

We must now concentrate on the other task we set ourselves, working out the Herbrand quotient of C_L. This is a difficult task to perform explicitly so we must try and use the properties of the Herbrand quotient to help us.

We make use of the fact that $J_L/L^\times E_L$ is isomorphic to the ideal class group of L (which is a finite group). A restatement of this shows that $L^\times E_L$ has finite index in J_L. But this implies that $L^\times E_L/L^\times$ has finite index as a subgroup of $C_L = J_L/L^\times$. So by the properties of the Herbrand quotient we must have that:

$$Q_G(C_L) = Q_G(L^\times E_L/L^\times).$$

But by the second isomorphism theorem we have that:

$$L^\times E_L/L^\times \cong E_L/(E_L \cap L^\times) \cong E_L/U_L,$$

where $U_L = \mathfrak{O}_L^\times$.

So we can see that:

$$Q_G(C_L) = Q_G(E_L/U_L).$$

Expanding E_L using the definition gives:

$$E_L = \prod_v \prod_{w|v} U_w = \prod_v U_{v,L}.$$

But we know that for a given place v of K, the group G permutes the places w lying above v. It follows that for each v the group $\prod_{w|v} U_w$ is a G module.

We would like to now be able to use the propety of the Herbrand quotient on products to be able to split the Herbrand quotient of E_L upto into lots of smaller Herbrand quotients (of the U_w groups). Unfortunately we cannot do this since we have an infinite product of groups.

To remove this obstacle we choose a finite set of places S of K and write:

$$E_L = \left(\prod_{v\in S}\prod_{w|v} U_w\right)\left(\prod_{v\notin S}\prod_{w|v} U_w\right) = \left(\prod_{v\in S} U_{v,L}\right)\left(\prod_{v\notin S} U_{v,L}\right).$$

It then follows that:

$$Q_G(E_L) = \prod_{v\in S}\left(Q_G\left(\prod_{w|v} U_w\right)\right) Q_G\left(\prod_{v\notin S}\prod_{w|v} U_w\right) = \prod_{v\in S}\left(Q_G\left(U_{v,L}\right)\right) Q_G\left(\prod_{v\notin S} U_{v,L}\right).$$

Finally, by Shapiro's lemma we have that $Q_G\left(\prod_{w|v} U_w\right) = Q_G\left(U_{v,L}\right) = Q_{G_w}(U_w)$ so we have that:

$$Q_G(E_L) = \left(\prod_{w\in S'} Q_{G_w}(U_w)\right) Q_G\left(\prod_{v\notin S}\prod_{w|v} U_w\right) = \left(\prod_{w\in S'} Q_{G_w}(U_w)\right) Q_G\left(\prod_{v\notin S} U_{v,L}\right),$$

where S' is a finite set of places of L chosen so that for every place $v \in S$ we have exactly one place $w \in S'$ lying above v.

With a special choice of S we will see that each Herbrand quotient here can be evaluated, enabling us to find the Herbrand quotient of E_L. This value coupled with the value of the Herbrand quotient of U_L will allow us to find the value of Herbrand quotient of E_L/U_L, giving us the value of Herbrand quotient of C_L (as above).

The result we need is the following:

Theorem 4.2.3. *Let L/K be a cyclic extension of number fields with Galois group G and let w be a place of L lying above a place v of K. Take S to be the set of infinite places of K along with the finite places of K corresponding to finite primes of K that ramify in L. Then:*

1. *if either w is finite, w is real infinite or v is complex infinite then $Q_{G_w}(U_w) = 1$;*
2. *if w is complex infinite but v is real infinite then $Q_{G_w}(U_w) = 2$;*
3. *for S as above we have that:*

$$Q_G\left(\prod_{v\notin S}\prod_{w|v} U_w\right) = Q_G\left(\prod_{v\notin S} U_{v,L}\right) = 1;$$

4. *we have that $Q_G(E_L) = 2^a$, where a is the number of real infinite places of K that extend to complex infinite places of L;*
5. *we have that $Q_G(U_L) = \frac{2^a}{[L:K]}$, where a is the same number as above.*

Proof. See p.94-p.96 of [2] for proof of the first three claims. To see the fourth claim we use the equality we had earlier:

$$Q_G(E_L) = \left(\prod_{w\in S'} Q_{G_w}(U_w)\right) Q_G\left(\prod_{v\notin S}\prod_{w|v} U_w\right) = \left(\prod_{w\in S'} Q_{G_w}(U_w)\right) Q_G\left(\prod_{v\notin S} U_{v,L}\right),$$

and use the previous three claims to simplify this. The only terms that have a Herbrand quotient contribution other than 1 to the product are the ones corresponding to complex infinite places of L that are extensions of real infinite places of K. These each contribute 2 to the product and the result follows.

The fifth claim is very difficult to prove. See p.96-p.100 of [2] for a proof of this. Essentially, we make a finite dimensional real vector space with formal basis elements indexed by the infinite places of L. Then we use Dirichlet's unit theorem along with logarithmic embeddings to translate into a lattice structure. The Herbrand quotient then becomes easier to calculate for this lattice.

□

We now have enough to work out the Herbrand quotient of C_L.

Corollary 4.2.4. *With the same conditions as above we have that:*

$$Q_G(C_L) = [L : K].$$

Proof. We already know that:

$$Q_G(C_L) = Q_G(E_L/U_L),$$

but using the previous theorem and the quotient property of the Herbrand quotient (U_L is a G-submodule of E_L) we find that:

$$Q_G(E_L/U_L) = \frac{Q_G(E_L)}{Q_G(U_L)} = \frac{2^a}{\frac{2^a}{[L:K]}} = [L : K].$$

□

Corollary 4.2.5. *(The global cyclic norm index inequality) If L/K is a cyclic extension of number fields and $\mathfrak{m}$ is a modulus of K that is divisible by a sufficiently high power of every ramified prime of L/K then:*

$$[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))] \geq [L : K].$$

Proof. We know that $Q_G(C_L) = [L : K]$. But by definition:

$$Q_G(C_L) = \frac{[C_L^G : \mathrm{im}(g_\sigma)]}{[\ker(g_\sigma) : \mathrm{im}(\sigma - 1)]} = \frac{[J_K : K^\times N_{L/K}(J_L)]}{[\ker(g_\sigma) : \mathrm{im}(\sigma - 1)]},$$

so that:

$$[L : K][\ker(g_\sigma) : \mathrm{im}(\sigma - 1)] = [J_K : K^\times N_{L/K}(J_L)].$$

This tells us that the degree $[L : K]$ divides the index $[J_K : K^\times N_{L/K}(J_L)]$.

Since this is a divisibility of positive integers we must have that:

$$[J_K : K^\times N_{L/K}(J_L)] \geq [L : K].$$

Now choose a complete modulus $\mathfrak{m}$ such that $K^\times N_{L/K}(J_L) \supseteq E_{K,\mathfrak{m}}$ (such a modulus exists by Corollary 4.2.2 and the discussion afterwards).

For this modulus we have that:

$$[J_K : K^\times N_{L/K}(J_L)] = [I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))],$$

giving the result. □

It has taken a lot of hard work to establish the two norm index inequalities. Now we can mix them together to see that for cyclic extensions L/K and for a sufficiently "big" complete modulus $\mathfrak{m}$ of K we have that:

$$[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))] = [L : K].$$

This result is by far the most important so far. It will allow us to prove the Artin reciprocity law in the next subsection.

4.3 Proving the Artin reciprocity law

Finally we get to prove the first of our two main theorems. This in itself will take quite a bit of work. We first have to start with a nice property of the restrictions of Artin symbols.

Lemma 4.3.1. *Let L/K be an Abelian extension of number fields and let E, F be two number fields lying in between K and L. Take a prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ that is unramified in L. Consider any triple of prime ideals $(\mathcal{P}_E, \mathcal{P}_F, \mathcal{P}_L)$ that come from the corresponding rings of integers $\mathfrak{O}_E, \mathfrak{O}_F, \mathfrak{O}_L$ and that all lie above $\mathfrak{p}$.*

Then:

$$\left(\frac{L/E}{\mathcal{P}_E}\right)\Big|_F = \left(\frac{F/K}{\mathfrak{p}}\right)^f = \left(\frac{F/K}{N_{E/K}(\mathcal{P}_E)}\right),$$

where f is the degree of the residue field $(\mathfrak{O}_E/\mathcal{P}_E)/(\mathfrak{O}_K/\mathfrak{p})$.

Proof. Given any $\alpha \in \mathfrak{O}_F$ the Artin symbol $\left(\frac{F/K}{\mathfrak{p}}\right)$ maps α as follows:

$$\left(\frac{F/K}{\mathfrak{p}}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathcal{P}_F.$$

Also the Artin symbol $\left(\frac{L/E}{\mathcal{P}_E}\right)$ behaves as follows:

$$\left(\frac{L/E}{\mathcal{P}_E}\right)(\beta) \equiv \beta^{N(\mathcal{P}_E)} \bmod \mathcal{P}_L,$$

for all $\beta \in \mathfrak{O}_L$.

If we restrict to F, taking $\beta \in \mathfrak{O}_F$ then we see that:

$$\left(\frac{L/E}{\mathcal{P}_E}\right)\Big|_F(\beta) \equiv \beta^{N(\mathcal{P}_E)} \bmod (\mathcal{P}_L \cap F).$$

But $\mathcal{P}_L \cap F = \mathcal{P}_F$ and so:

$$\left(\frac{L/E}{\mathcal{P}_E}\right)\Big|_F(\beta) \equiv \beta^{N(\mathcal{P}_E)} \bmod \mathcal{P}_F.$$

Since $\mathfrak{p}^f = \mathcal{P}_E$ we note that:

$$\left(\frac{F/K}{\mathfrak{p}}\right)^f(\alpha) \equiv \alpha^{N(\mathfrak{p})^f} \equiv \alpha^{N(\mathfrak{p}^f)} \equiv \alpha^{N(\mathcal{P}_E)} \bmod \mathcal{P}_F,$$

for all $\alpha \in \mathfrak{O}_F$, giving $\left(\frac{F/K}{\mathfrak{p}}\right)^f = \left(\frac{F/K}{N_{E/K}(\mathcal{P}_E)}\right) = \left(\frac{L/E}{\mathcal{P}_E}\right)\Big|_F$. □

Note that the above can be extended by multiplicativity to fractional ideals. Let $\mathfrak{m}_E$ be a modulus of $\mathfrak{O}_E$ that is divisible by all primes of E that are ramified in L. Then for any $\mathfrak{a} \in I_E(\mathfrak{m}_E)$ we have that:

$$\left(\frac{L/E}{\mathfrak{a}}\right)\Big|_F = \left(\frac{F/K}{N_{E/K}(\mathfrak{a})}\right).$$

We note the following corollary:

Corollary 4.3.2. *With the above notation we have that:*

$$\left(\frac{L/K}{\mathfrak{p}}\right)\Big|_F = \left(\frac{F/K}{\mathfrak{p}}\right)$$

$$\left(\frac{L/E}{\mathcal{P}_E}\right) = \left(\frac{L/K}{N_{E/K}(\mathcal{P}_E)}\right)$$

Proof. For the first, take $E = K$ in the above lemma (since then $\mathfrak{p} = \mathcal{P}_E$). For the second take $L = F$ in the above lemma (the restriction to F is then not needed). □

The results above are really important since they will let us jump between the Artin maps of related extensions.

One even more important (but simple) corollary of the above is the following:

Corollary 4.3.3. *For any Abelian extension L/K and any complete modulus $\mathfrak{m}$ for L/K we have that:*

$$N_{L/K}(I_L(\mathfrak{m})) \subseteq \ker(\Phi_{L/K,\mathfrak{m}}).$$

Proof. Fix a complete modulus $\mathfrak{m}$ for L/K and choose any prime ideal $\mathcal{P}_L$ of $\mathfrak{O}_L$ that does not lie above any prime ideal in $\mathfrak{m}$ (i.e.$\mathcal{P}_L$ is coprime to $\mathfrak{m}_0\mathfrak{O}_L$). Then $\mathcal{P}_L$ is unramified in L. By the restriction properties of the Artin symbol above (taking $L = E = F$) we have that:

$$\left(\frac{L/K}{N_{L/K}(\mathcal{P}_L)}\right) = \left(\frac{L/L}{\mathcal{P}_L}\right)\Big|_L$$

but $\mathrm{Gal}(L/L)$ only has one element, the identity automorphism of L (denoted by 1).

Thus $\left(\frac{L/K}{N_{L/K}(\mathcal{P}_L)}\right) = 1$ and so the norms of all such prime ideals lie in the kernel of the Artin map (they each have trivial Artin symbol).

It is now obvious that $\left(\frac{L/K}{N_{L/K}(\mathfrak{a})}\right) = 1$ for any $\mathfrak{a} \in I_L(\mathfrak{m})$ by multiplicativity of the norm and the Artin symbol (along with unique factorisation of $\mathfrak{a}$ into prime ideals). This gives the result. □

We now start our proof of Artin reciprocity. We start with the proof that the Artin map is surjective.

Theorem 4.3.4. *Given an Abelian extension L/K and any complete modulus $\mathfrak{m}$ for L/K we have that the Artin map $\Phi_{L/K,\mathfrak{m}}$ is surjective.*

Proof. Firstly we note that in cyclic extensions E/F of degree more than 1 there are infinitely many primes of F that do not split completely in E. For a proof of this see p.194 of [1] (it uses the Artin-Whaples approximation theorem, which is closely related to the Chinese remainder theorem).

Denote by H the image of the Artin map $\Phi_{L/K,\mathfrak{m}}$ (so that H is a subgroup of $\mathrm{Gal}(L/K)$). Now by the Galois correspondence, H has a fixed field M lying between K and L. We prove that $M = K$ and then by the Galois correspondence we must have that $H = \mathrm{Gal}(L/K)$ (since L/K is Galois by assumption). Finally this will tell us that the Artin map is surjective.

Taking a prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ coprime to $\mathfrak{m}$, the claim is that $\mathfrak{p}$ splits completely in M. Suppose not, then $\left(\frac{M/K}{\mathfrak{p}}\right)$ is not the identity automorphism in $\mathrm{Gal}(M/K)$.

But $\left(\frac{M/K}{\mathfrak{p}}\right) = \left(\frac{L/K}{\mathfrak{p}}\right)\Big|_M$ by the previous corollary, thus $\left(\frac{L/K}{\mathfrak{p}}\right) \in H$ does not fix M. This is a contradiction, so all such $\mathfrak{p}$ split completely in M.

Now we see that only finitely many primes of K do not split completely in M (the ones that divide $\mathfrak{m}$). However, this does not yet prove our claim since M/K is an Abelian extension and we can only use the result mentioned above when working in cyclic extensions. We create one now.

Suppose that $M \neq K$. Then $[M : K] > 1$ and so we can find a field M_0 lying between K and M such that M_0/K is cyclic of degree more than 1 (this is true by the theory of field extensions). Since M_0 is contained in M and $[M_0 : K] > 1$, we still have that only finitely many primes of K can split completely in M_0. This is the contradiction we needed thus $M = K$ and the result is proved. □

Now that we have the surjectivity of the Artin map for any complete modulus, we work on proving the second part of the Artin reciprocity theorem (Theorem 2.3.1). Our strategy is quite long-winded. The general idea is as follows:

1. Show that the second part of the Artin reciprocity theorem holds for cyclotomic extensions $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. This case was tackled in the Semester 1 project.

   We actually showed that $\ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},(m)\infty}) = P_{\mathbb{Q},1}((m)\infty)$ here so the modulus $(m)\infty$ does the trick. The justification that the exact kernel is given in terms of norms will be ignored for now as this will come for free when we get to the third stage of our strategy.

2. Use this result to help prove the second part of Artin reciprocity for extensions of the form $K(\zeta_m)/K$ where K is a number field (this then makes the result true for any extension L/K of number fields such that $K \subseteq L \subseteq K(\zeta_m)$).

3. Find a way to deduce from this the result for a general cyclic extension L/K (this will take the most work and will rely on a chain of lemmas). We prove this in a counter-intuitive way to what would be expected.

4. Finally, deduce the result for Abelian extensions L/K as a simple corollary.

Since stage one has already been considered in Semester 1 (and is not too difficult to do should the reader have limited or no access to the other project) we can move on to stage two.

Theorem 4.3.5. *Let K be a number field and L be a field such that $K \subseteq L \subseteq K(\zeta_m)$ for some mth root of unity ζ_m. Then there exists a complete modulus $\mathfrak{m}$ of L/K such that $P_{K,1}(\mathfrak{m}) \subseteq \ker(\Phi_{L/K,\mathfrak{m}})$.*

Proof. We prove the case where $L = K(\zeta_m)$ for some mth root of unity ζ_m. The full result will follow by restriction properties of the Artin symbol. To see this note that if L is strictly contained in $K(\zeta_m)$ for some m then we can restrict the Artin symbols with respect to $K(\zeta_m)/K$ to get Artin symbols with respect to the extension L/K. The result will then follow for the same modulus.

So consider the extension $K(\zeta_m)/K$ and let $\mathfrak{m}_\infty$ denote the formal product of all distinct real embeddings of K (it can be assumed that $m > 2$). We show that the modulus $(m)\mathfrak{m}_\infty$ is such that $P_{K,1}((m)\mathfrak{m}_\infty) \subseteq \ker(\Phi_{K(\zeta_m)/K,(m)\mathfrak{m}_\infty})$. This modulus is certainly a complete modulus for the extension since the only primes that ramify here are the ones dividing m ($L \supset \mathbb{R}$ here and so none of the real infinite primes ramify here).

Take $\mathfrak{a} \in P_{K,1}((m)\mathfrak{m}_\infty)$, then $\mathfrak{a} = (\alpha)$ for some $\alpha \in K^\times$ such that $\alpha \equiv 1 \bmod (m)$ and $\sigma(\alpha) > 0$ for all real embeddings σ of K.

Using Lemma 4.3.1 we see that:

$$\left(\frac{K(\zeta_m)/K}{\mathfrak{a}}\right)\Big|_{\mathbb{Q}(\zeta_m)} = \left(\frac{K(\zeta_m)/K}{(\alpha)}\right)\Big|_{\mathbb{Q}(\zeta_m)} = \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{N_{K/\mathbb{Q}}((\alpha))}\right) = \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{(N(\alpha))}\right),$$

where $N(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(\alpha)$ is the usual norm of an element.

Now since $\sigma(\alpha) > 0$ for all real embeddings σ of K, we have that $N(\alpha) > 0$ (all of the other $\sigma(\alpha)$ terms can be paired off in complex conjugate paire to make positive products). Also since $\alpha \equiv 1 \bmod (m)$ we have that $N(\alpha) \equiv 1 \bmod m$. Thus $(N(\alpha)) \in P_{\mathbb{Q},1}((m)\infty)$, where (m) is now the ideal generated by m in $\mathbb{Z}$. But we have already proved Artin reciprocity for the extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ and so we know that $P_{\mathbb{Q},1}((m)\infty) = \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},(m)\infty})$. This tells us that $(N(\alpha)) \in \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},(m)\infty})$.

Thus:

$$\left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{(N(\alpha))}\right) = 1,$$

meaning that:

$$\left(\frac{K(\zeta_m)/K}{\mathfrak{a}}\right)\Big|_{\mathbb{Q}(\zeta_m)} = 1.$$

Finally, an element of $\mathrm{Gal}(K(\zeta_m)/K)$ is the identity if and only if its restriction to $\mathbb{Q}(\zeta_m)$ is the identity. This is because such automorphisms are determined completely by their action on ζ_m. Thus we must have that:

$$\left(\frac{K(\zeta_m)/K}{\mathfrak{a}}\right) = 1,$$

and so $\mathfrak{a} \in \ker(\Phi_{K(\zeta_m)/K,(m)\mathfrak{m}_\infty})$. □

This result solves stage two and now we move on to the more substantial stage three. The proof of this result for general cyclic extensions L/K will be proved in a different way. Instead, we prove that there exists a complete modulus $\mathfrak{m}$ for L/K that satisfies $\ker(\Phi_{L/K,\mathfrak{m}}) \subseteq P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$. We may assume also that $\mathfrak{m}$ is such that $K^\times N_{L/K}(J_L) \supseteq E_{K,\mathfrak{m}}$.

To see how these facts combine to imply that $P_{K,1}(\mathfrak{m}) \subseteq \ker(\Phi_{L/K,\mathfrak{m}})$, we first note that such a modulus was proven to exist earlier and that for all such moduli we have:

$$[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})N_{L/K}(\mathfrak{m})] = [L : K] = |\mathrm{Gal}(L/K)|$$

(by using both of the norm index inequalities; we are working in a cyclic extension here and $\mathfrak{m}$ is the special kind of modulus, so both inequalities certainly apply).

On the other hand, we know that the Artin map $\Phi_{L/K,\mathfrak{m}}$ is surjective and so also:

$$[I_K(\mathfrak{m}) : \ker(\Phi_{L/K,\mathfrak{m}})] = |\mathrm{Gal}(L/K)|,$$

giving the equality:

$$[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})N_{L/K}(\mathfrak{m})] = [I_K(\mathfrak{m}) : \ker(\Phi_{L/K,\mathfrak{m}})].$$

The fact that $\ker(\Phi_{L/K,\mathfrak{m}}) \subseteq P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$ would then guarantee that:

$$\ker(\Phi_{L/K,\mathfrak{m}}) = P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m})),$$

which certainly contains $P_{K,1}(\mathfrak{m})$.

So we have found another theorem that gives the result that we want as a direct consequence (using all of the major results and ideas we have covered so far in this project). We will see that this theorem is easier to prove than the original one. Note also that if we can prove this new theorem we also get the final part of Artin reciprocity for free (the explicit form of the Artin kernel in terms of norm groups).

However, this new theorem is not entirely easy to prove. We want to somehow be able to relate the general cyclic case to the case we had above, where L is such that $K \subseteq L \subseteq K(\zeta_m)$. This is exactly what we do, although we first have to be able to construct nice cyclotomic extensions. In order to do this properly so that the extensions do not interfere with each other too much we need a chain of interesting lemmas, each one building on the one before it.

The first lemma comes from elementary number theory. Basically it states that every integer bigger than 1 can be made to have a given prime power order mod p for some rational prime p.

Lemma 4.3.6. *Let $a, r > 1$ be integers and let q be a rational prime. Then there exists a rational prime p such that a mod p has order q^r (i.e. the class $[a]$ has order q^r in the group $(\mathbb{Z}/p\mathbb{Z})^\times$).*

Proof. We go for a clever divisibility proof. Define:

$$T = \frac{a^{q^r} - 1}{a^{q^{r-1}} - 1}.$$

Now suppose that p is a rational prime such that $p|T$ and $p \nmid (a^{q^{r-1}} - 1)$. Then it follows that $a^{q^r} \equiv 1 \bmod p$ and also that $a^{q^{r-1}} \not\equiv 1 \bmod p$, showing that a mod p has order q^r (if it had a lower order then it would be a lower power of q by Lagrange, but this contradicts the second congruence).

It now remains to prove that such a prime p exists. We can expand T to give:

$$T = (a^{q^{r-1}} - 1)^{q-1} + q(a^{q^{r-1}} - 1)^{q-2} + \ldots + q(a^{q^{r-1}} - 1) + q.$$

This shows that the only rational prime to divide both T and $(a^{q^{r-1}} - 1)$ must divide q, and so must be equal to q. Thus it suffices to prove that T is not a power of q since then there will exist a prime p distinct from q that gives the result.

Certainly $T \neq q$ since $1 < q < T$, so that we only have to show that T is not a higher power of q. In order to do this we show that T is not divisible by q^2.

For the case $q > 2$ we have via the expansion above that $T \equiv q \bmod q^2$ so that $q^2 \nmid T$ (the condition $q > 2$ is there to make sure that there are at least 3 terms in the expansion).

Finally the case $q = 2$ gives that $T = (a^{2^{r-1}} - 1) + 2 = a^{2^{r-1}} + 1$ and clearly $2^2 = 4$ does not divide this (since then $(a^{2^{r-2}})^2 \equiv 3 \bmod 4$, implying that 3 is a quadratic residue mod 4). □

Actually, if we instead consider primes p such that $a \bmod p$ has order *divisible* by a fixed q^r we find that there must be infinitely many and that we can find such a p that is arbitrarily large.

To see this, note that by the above lemma there exists an infinite set of primes $P = \{p_i \mid i \in \mathbb{N}\}$ such that $a \bmod p_i$ has order q^{r+i}. Clearly for each $p_i \in P$ we have that the order of $a \bmod p_i$ is divisible by q^r and so there are infinitely many such primes. Since the number of primes less than a given positive bound is finite, we conclude that the primes in P get arbitrarily large.

We now consider a more general case than prime power orders.

Corollary 4.3.7. *Let $a, n > 1$ be integers. Then there exists an integer $d > 1$ such that $a \bmod d$ has order divisible by n (i.e. the class $[a]$ has order divisible by n in the group $(\mathbb{Z}/d\mathbb{Z})^\times$).*

Moreover, d can be taken to have all of its prime divisors being arbitrarily large.

Proof. We start by factorising n into prime powers:

$$n = q_1^{r_1} q_2^{r_2} \dots q_t^{r_t}.$$

By the above discussion, there exists for each j a prime p_j such that $a \bmod p_j$ has order divisible by $q_j^{r_j}$. Then by taking $d = p_1 p_2 \dots p_t$ we see that $a \bmod d$ has order divisible by $q_1^{r_1} q_2^{r_2} \dots q_t^{r_t} = n$.

Since each of the primes p_j can be made arbitrarily large, the second claim also follows. □

The above result is needed to prove a more useful lemma. First we make a definition:

Definition 4.3.8. Two integers a, b are said to be *independent* mod n if the group generated by $[a]$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ shares only the element $[1]$ with the group generated by $[b]$ in $(\mathbb{Z}/n\mathbb{Z})^\times$.

We now have the following:

Lemma 4.3.9. *Let $a, n > 1$ be integers. Then there exist positive integers b, m such that:*

1. *the order of a mod m is divisible by n, and m can be taken to have all of its prime divisors being arbitrarily large (i.e. m satisfies the role of d in the above corollary);*
2. *the order of b mod m is also divisible by n;*
3. *the integers a and b are independent mod m.*

Proof. By the above corollary, we can find a positive integer d such that the first condition is satisfied (for d in place of m). Unfortunately not all such d satisfy the other two conditions. However, we can construct an m that does work using a fixed d.

Suppose that n' is the order of $a \bmod d$ (so that $n | n'$). We can use the corollary again to find a positive integer d' such that $a \bmod d'$ has order divisible by n' (and d' can be taken to have prime divisors distinct from d by making them arbitrarily larger than those of d).

If we define $m = dd'$ then we shall see that this m does the job. We have yet to make our choice of b. Using the Chinese remainder theorem we can choose b to be a solution to the congruences:

$$b \equiv a \bmod d$$

$$b \equiv 1 \bmod d'$$

since then we see that $b \bmod m$ has the same order as $a \bmod d$ (which has order divisible by n).

It remains to check independence. Suppose that a and b are not independent mod m. Then there exists integers i, j such that $a^i \equiv b^j \bmod m$ (with neither of $a^i, b^j \equiv 1 \bmod m$).

Working mod d' instead we see that $a^i \equiv b^j \equiv 1 \bmod d'$, since $b \equiv 1 \bmod d'$. But we know that the order of $a \bmod d'$ is divisible by n', so that $n' | i$. Also n' is the order of $a \bmod d$ so that $a^i \equiv 1 \bmod d$.

Together, the congruences:

$$a^i \equiv 1 \bmod d$$

$$a^i \equiv 1 \bmod d'$$

give that $a^i \equiv 1 \bmod m$. This is clearly a contradiction. □

Given that cyclotomic extensions of the form $K(\zeta_m)/K$ have Galois groups isomorphic to subgroups of $(\mathbb{Z}/m\mathbb{Z})^\times$, it should be no surprise that we can now link the above result to Artin symbols of $K(\zeta_m)/K$. In order to make this work smoothly we need to create an extension $K(\zeta_m)/K$ that has the biggest Galois group possible.

Lemma 4.3.10. *Let K be a number field and $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$. For any integer $n > 1$ we can find a positive integer m coprime to $\mathfrak{p}$ (that has all prime divisors arbitrarily large) and a primitive mth root of unity ζ_m such that:*

1. *the extension $K(\zeta_m)/K$ satisfies $\mathrm{Gal}(K(\zeta_m)/K) \cong (\mathbb{Z}/m\mathbb{Z})^\times$;*
2. *the Artin symbol $\left(\frac{K(\zeta_m)/K}{\mathfrak{p}}\right)$ has order divisible by n in $\mathrm{Gal}(K(\zeta_m)/K)$;*
3. *there exists $\tau \in \mathrm{Gal}(K(\zeta_m)/K)$ having order divisible by n such that τ is independent of $\left(\frac{K(\zeta_m)/K}{\mathfrak{p}}\right)$ in the group $\mathrm{Gal}(K(\zeta_m)/K)$ (i.e. independent when considered as elements of $(\mathbb{Z}/m\mathbb{Z})^\times$ under the isomorphism above).*

Proof. We take $a = N(\mathfrak{p})$ in the previous lemma (where $N(\mathfrak{p}) = |\mathfrak{O}_K/\mathfrak{p}| \in \mathbb{Z}$ is the absolute norm of $\mathfrak{p}$). Thus, given a positive integer n we can find a positive integer m such that $N(\mathfrak{p}) \bmod m$ has order divisible by n. Also we can find an integer b such that $b \bmod m$ has order divisible by n and that $N(\mathfrak{p}), b$ are independent mod m.

By the fact that the prime factors of m can be made arbitrarily large, we take m to be divisible by none of the rational primes that ramify in K (of which there are only finitely many), nor the rational prime lying below $\mathfrak{p}$.

We now have that $K \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$. To see this note that only the rational primes dividing m can ramify in $\mathbb{Q}(\zeta_m)$, thus only these primes can ramify in $K \cap \mathbb{Q}(\zeta_m)$ (since it is a subfield of $\mathbb{Q}(\zeta_m)$). By the choice of m no rational primes dividing m ramify in K, thus none of the rational primes dividing m ramify in $K \cap \mathbb{Q}(\zeta_m)$ (since it is a subfield of K). Thus $K \cap \mathbb{Q}(\zeta_m)$ is an extension field of $\mathbb{Q}$ that is unramified everywhere. The only such field is $\mathbb{Q}$ itself, thus $K \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$.

Now by Galois theory we must have that:

$$\mathrm{Gal}(K(\zeta_m)/K) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/(K \cap \mathbb{Q}(\zeta_m))) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times,$$

the isomorphism being given by restriction to $\mathbb{Q}(\zeta_m)$. Thus the first condition is satisfied for the m we have constructed.

Carrying out the above isomorphism on the Artin symbol $\left(\frac{K(\zeta_m)/K}{\mathfrak{p}}\right)$ gives:

$$\left(\frac{K(\zeta_m)/K}{\mathfrak{p}}\right) \longleftrightarrow \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{N(\mathfrak{p})}\right) \longleftrightarrow [N(\mathfrak{p})].$$

Since $[N(\mathfrak{p})] = [a]$ has order divisible by n in $(\mathbb{Z}/m\mathbb{Z})^\times$ we must have, by the isomorphism above, that $\left(\frac{K(\zeta_m)/K}{\mathfrak{p}}\right)$ has order divisible by n in $\mathrm{Gal}(K(\zeta_m)/K)$. This satisfies the second condition.

Finally choose τ such that under the above isomorphism $\tau \longleftrightarrow [b]$ (where b is the integer found above). Then, since $N(\mathfrak{p}), b$ are independent mod m we must have that $\left(\frac{K(\zeta_m)/K}{\mathfrak{p}}\right)$ and τ are independent in $\mathrm{Gal}(K(\zeta_m)/K)$. The third condition is satisfied and we are done. □

Now we reach the most important lemma. After this we will be able to prove the remaining part of the Artin reciprocity theorem. In fact the result we need is due to Artin himself and essentially makes use of the nicely behaved cyclotomic extension we have just shown to exist. The following lemma will guarantee that for cyclic extensions L/K there is an even nicer behaved cyclotomic extension of K that does not interfere with L too much.

Lemma 4.3.11. *(Artin's lemma) Let L/K be a finite cyclic extension of number fields and $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$. Then there exists a positive integer m coprime to $\mathfrak{p}$ (having all of its prime factors being arbitrarily large), a primitive mth root of unity ζ_m and a field E containing K such that:*

1. *the fields L and $K(\zeta_m)$ have only the elements of K in common, i.e. $L \cap K(\zeta_m) = K$;*
2. *the prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ splits completely in E;*
3. *the fields L and E have only the elements of K in common, i.e. $L \cap E = K$;*
4. *adjoining ζ_m to L is the same as adjoining ζ_m to E, i.e. $E(\zeta_m) = L(\zeta_m)$.*

Proof. Use $n = [L : K]$ in the previous lemma and take the integer m to be such that it is not divisible by any rational primes that ramify in L, along with the condition that m is coprime to $\mathfrak{p}$.

Then by the previous lemma we have that $\mathrm{Gal}(K(\zeta_m)/K) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ and that the order of $\left(\frac{K(\zeta_m)/K}{\mathfrak{p}}\right)$ in $\mathrm{Gal}(K(\zeta_m)/K)$ is divisible by n.

Similar ramification arguments to earlier tell us that $K \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$, $L \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$ and $L \cap K(\zeta_m) = K$. Thus the first condition is satisfied.

We now work on constructing the field E. Since L and $K(\zeta_m)$ have only elements from the field K in common, we find the isomorphism of Galois groups:

$$\mathrm{Gal}(L(\zeta_m)/K) \cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(K(\zeta_m)/K),$$

which works by restiction to L for the first component and restriction to $K(\zeta_m)$ for the second.

But L/K is cyclic so $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ for some $\sigma \in \mathrm{Gal}(L/K)$. Also, by the construction of m we know that $\mathrm{Gal}(K(\zeta_m)/K) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

Thus we have that:

$$\mathrm{Gal}(L(\zeta_m)/K) \cong \langle\sigma\rangle \times (\mathbb{Z}/m\mathbb{Z})^\times.$$

For simplicity we identify both sides of this isomorphism. Under this convention we can write:

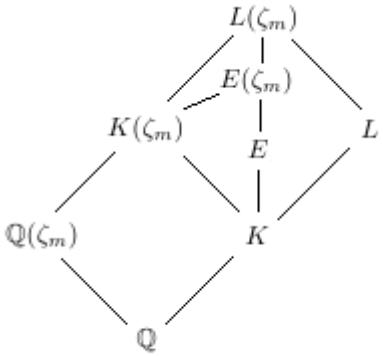
$$\left(\frac{L(\zeta_m)/K}{\mathfrak{p}}\right) = \left(\frac{L/K}{\mathfrak{p}}\right) \times \left(\frac{K(\zeta_m)/K}{\mathfrak{p}}\right),$$

by using restriction properties of the Artin map.

Now take $\tau \in \mathrm{Gal}(K(\zeta_m)/K)$ as in the previous lemma and consider the subgroup H of $\mathrm{Gal}(L(\zeta_m)/K)$ generated by the elements $\sigma \times \tau$ and $\left(\frac{L/K}{\mathfrak{p}}\right) \times \left(\frac{K(\zeta_m)/K}{\mathfrak{p}}\right)$.

Let E be the fixed field of H (so that E is contained in $L(\zeta_m)$). We aim to show that this field satisfies the other conditions.

Here is the field diagram:



We know that the Artin symbol $\left(\frac{L(\zeta_m)/K}{\mathfrak{p}}\right)$ generates the decomposition group of $\mathfrak{p}$ with respect to the extension $L(\zeta_m)/K$. By the convention above we see that H must contain this decomposition group since

$\left(\frac{L(\zeta_m)/K}{\mathfrak{p}}\right)$ is one of the generators for H. But by the order reversing property of the Galois correspondence, this tells us that E is contained within the decomposition field of $\mathfrak{p}$ in $L(\zeta_m)/K$ (i.e. the fixed field corresponding to the decomposition group itself).

It is generally known that the prime ideal $\mathfrak{p}$ splits completely in any extension field of K contained within the decomposition field of $\mathfrak{p}$. Thus the second condition is certainly satisfied for our choice of E.

Now we work on proving the third condition. Note that by definition we have $\sigma \times \tau \in H$, thus $\sigma \times \tau$ fixes E. Now $L \cap E$ is a subfield of E and so the elements of this field are also fixed by H. Also the element $1 \times \tau \in \mathrm{Gal}(L(\zeta_m)/K)$ fixes L under the identification above. To see this recall that $L \cap K(\zeta_m) = K$ so that with respect to the field L, the τ component only acts on those elements of L that lie in $K(\zeta_m)$, which are elements of K and so are fixed anyway. Thus using the fact that $L \cap E$ is a subfield of L we must have that $1 \times \tau$ fixes $L \cap E$ too.

This tells us that actually the automorphism $\sigma \times 1 \in \mathrm{Gal}(L(\zeta_m)/K)$ must fix $L \cap E$ (since in the whole Galois group we have that $\sigma \times 1 = (\sigma \times \tau)(1 \times \tau)^{-1}$). But σ generates $\mathrm{Gal}(L/K)$ and so $L \cap E$ is fixed by the whole of $\mathrm{Gal}(L/K)$ (this is exactly where the cyclic nature of L/K is needed since this would not follow otherwise). Thus by the Galois correspondence we have that $L \cap E = K$.

It remains to prove the last condition. Since E is by definition the fixed field of H, we have that $H \cong \mathrm{Gal}(L(\zeta_m)/E)$. Also it is easy to see that:

$$\mathrm{Gal}(L(\zeta_m)/K(\zeta_m)) \cong \mathrm{Gal}(L/K) \times 1,$$

since the automorphisms on the right are the only ones that can fix $K(\zeta_m)$.

By these two facts we find that the group $H \cap (\mathrm{Gal}(L/K) \times 1)$ has fixed field $E(\zeta_m)$ (by the order reversing property of the Galois correspondence it must be the smallest field containing both E and $K(\zeta_m)$). We show that actually $H \cap (\mathrm{Gal}(L/K) \times 1)$ is the trivial group and is equal to $\mathrm{Gal}(L(\zeta_m)/K(\zeta_m))$, thus showing that $L(\zeta_m) = K(\zeta_m)$.

To do this, take $\gamma \in H \cap (\mathrm{Gal}(L/K) \times 1)$. Then:

$$\gamma = (\sigma \times \tau)^i \left(\left(\frac{L/K}{\mathfrak{p}} \right) \times \left(\frac{K(\zeta_m)/K}{\mathfrak{p}} \right) \right)^j = \sigma^i \left(\frac{L/K}{\mathfrak{p}} \right)^j \times \tau^i \left(\frac{K(\zeta_m)/K}{\mathfrak{p}} \right)^j$$

and also:

$$\gamma = \sigma^k \times 1$$

for some integers i, j and k.

From this we can see that (by comparing the second components):

$$\tau^i \left(\frac{K(\zeta_m)/K}{\mathfrak{p}} \right)^j = 1.$$

But τ and $\left(\frac{K(\zeta_m)/K}{\mathfrak{p}}\right)$ are independent (in the sense of the previous lemma) and both have order divisible by n. Thus $n|i$ and $n|j$.

Now compare the first components to find that:

$$\sigma^i \left(\frac{L/K}{\mathfrak{p}} \right)^j = \sigma^k.$$

But both i and j are divisible by $n = [L : K] = |\mathrm{Gal}(L/K)|$, so that $\sigma^i \left(\frac{L/K}{\mathfrak{p}}\right)^j = 1$ in $\mathrm{Gal}(L/K)$. Hence $b = \sigma^a \times 1 = 1 \times 1$, showing that $H \cap (\mathrm{Gal}(L/K) \times 1) \cong \mathrm{Gal}(L(\zeta_m)/K(\zeta_m))$ is trivial. □

With Artin's lemma at our disposal we can finally prove the rest of the Artin reciprocity law. Essentially we use Artin's lemma multiple times to gain the existence of a list of positive integers and a list of extension fields. Using these we construct a bigger extension of K that turns the situation into the cyclotomic one we had before.

Recall that earlier we reduced the rest of Artin reciprocity to:

Theorem 4.3.12. *Let L/K be a finite cyclic extension of number fields of degree n whose Galois group is generated by σ. Then $\ker(\Phi_{L/K,\mathfrak{m}}) \subseteq P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$ for some complete modulus $\mathfrak{m}$ of L/K such that $K^\times N_{L/K}(J_L) \supseteq E_{K,\mathfrak{m}}$.*

Proof. Choose the complete modulus $\mathfrak{m}$ to be a multiple of the conductor $\mathfrak{f}$ of the extension L/K (defined earlier). So $\mathfrak{m}$ is divisible only by primes of K that ramify in L and all such primes divide $\mathfrak{m}$. We show that the result is true for this modulus. Take any ideal $\mathfrak{a} \in \ker(\Phi_{L/K,\mathfrak{m}})$. It is our aim to show that $\mathfrak{a}$ can be written as something in $P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$.

Firstly we factorise $\mathfrak{a}$ into prime ideals of $\mathfrak{O}_K$:

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{\gamma_i},$$

where each $\gamma_i \in \mathbb{Z}$.

Now since L/K is cyclic we have integers d_i such that:

$$\left(\frac{L/K}{\mathfrak{p}^{\gamma_i}}\right) = \sigma^{d_i},$$

for each i.

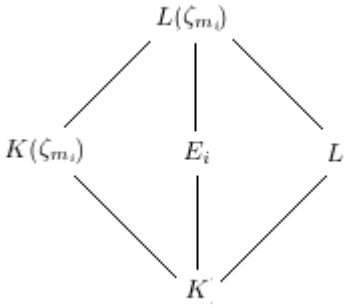
By multiplicativity of the Artin symbol, it now follows that:

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \sigma^{d_1+d_2+\ldots d_r}.$$

But $\mathfrak{a}$ lies in the Artin kernel, so actually $\left(\frac{L/K}{\mathfrak{a}}\right) = 1$, which in turn implies that $n|(d_1 + d_2 + \ldots d_r)$.

Now we use Artin's lemma with respect to the r prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ to get integers $m_1, m_2, \ldots, m_r$ and fields $E_1, E_2, \ldots, E_r$, each satisfying the conditions in Artin's lemma. The corresponding roots of unity are denoted $\zeta_{m_1}, \zeta_{m_2}, \ldots, \zeta_{m_r}$ (so that each ζ_{m_i} is a primitive m_ith root of unity). Note that we can take the integers m_i to be pairwise coprime. Also we can assume that they are coprime to the primes of $\mathbb{Q}$ that ramify in K and coprime to the prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ (this is all possible by the arbitrary nature of the prime factors of the integers m_i). As a consequence of this, the ideal $\mathfrak{a}$ is actually coprime to $m_1 m_2 \ldots m_r \mathfrak{m}$.

We have, for each i, the following diagram:



Let $E = E_1 E_2 \ldots E_r$, i.e. the compositum of the E_i then by Artin's lemma we have that $L \cap E_i = K$ for all i.

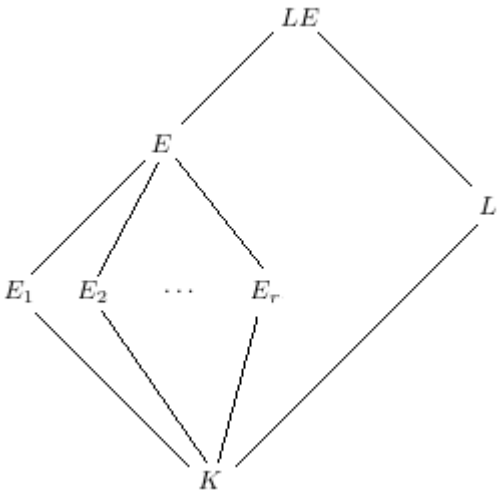
Also, similar to the proof of the last lemma we have that:

$$\mathrm{Gal}(L(\zeta_1, \zeta_2, \ldots, \zeta_r)/K) \cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(K(\zeta_1)/K) \times \mathrm{Gal}(K(\zeta_2)/K) \times \ldots \times \mathrm{Gal}(K(\zeta_r)/K).$$

By generalising the argument in the proof of Artin's lemma it is possible to see that $L \cap E = K$ (by forming the subgroup generated by certain products of Artin symbols and the generator of $\mathrm{Gal}(L/K)$). This observation tells us that:

$$\mathrm{Gal}(LE/E) \cong \mathrm{Gal}(LE_1/E_1) \cong \mathrm{Gal}(LE_2/E_2) \cong \ldots \mathrm{Gal}(LE_r/E_r) \cong \mathrm{Gal}(L/K),$$

the isomorphism given via restriction of automorphisms. This is a very nice situation to be in and will allow us to finish the proof in a nicer realm.



Now choose $\mathfrak{b} \in I_E(m_1 m_2 \dots \mathfrak{m}\mathfrak{O}_E)$ such that $\left(\frac{LE/E}{\mathfrak{b}}\right)\Big|_L = \sigma$. In other words we choose $\mathfrak{b}$ to be coprime to all of the m_i and to the ideal $\mathfrak{m}\mathfrak{O}_E$ (also chosen so that its Artin symbol in LE/E restricts in L to give σ). Such a $\mathfrak{b}$ exists by surjectivity of the Artin map.

Then:

$$\left(\frac{L/K}{N_{E/K}(\mathfrak{b})}\right) = \left(\frac{LE/E}{\mathfrak{b}}\right)\Big|_L = \sigma.$$

But then:

$$\left(\frac{L/K}{\mathfrak{p}_i^{\gamma_i}(N_{E/K}(\mathfrak{b}))^{-d_i}}\right) = \sigma^{d_i}\sigma^{-d_i} = 1,$$

for all i.

Now by construction we have that each $\mathfrak{p}_i$ splits completely in E_i. Note that this means that given any prime ideal $\mathcal{P}_i$ of $\mathfrak{O}_{E_i}$ lying above $\mathfrak{p}_i$, we have that $N_{E_i/K}(\mathcal{P}_i) = \mathfrak{p}_i$ (since $\mathfrak{p}_i$ splits completely so we have that $e = f = 1$, where e is the corresponding ramification index and f is the residue field degree). All that is important here is that $\mathfrak{p}_i$ is the norm of some prime ideal of $\mathfrak{O}_{E_i}$.

But then we must have that $\mathfrak{p}_i^{\gamma_i}(N_{E/K}(\mathfrak{b}))^{-d_i}$ is the norm of some fractional ideal $\mathfrak{C}_{E_i}$ of E_i (by multiplicativity of the norm and by noting that a norm relative to E/K can be made into a norm relative to E_i/K by restriction). Note that actually $\mathfrak{C}_{E_i}$ can be taken to be coprime to m_i and to $\mathfrak{m}$.

Given the above and the restriction properties of the Artin symbol we can now write:

$$\left(\frac{LE_i/E_i}{\mathfrak{C}_{E_i}}\right)\Big|_L = \left(\frac{L/K}{\mathfrak{p}_i^{\gamma_i}(N_{E/K}(\mathfrak{b}))^{-d_i}}\right) = 1.$$

But we know that $\mathrm{Gal}(KE_i/E_i) \cong \mathrm{Gal}(L/K)$ and so actually:

$$\left(\frac{LE_i/E_i}{\mathfrak{C}_{E_i}}\right) = 1,$$

telling us that $\mathfrak{C}_{E_i}$ is in the kernel of the corresponding Artin map with respect to extension LE_i/E_i and modulus $m_i\mathfrak{m}\mathfrak{O}_{E_i}$.

Now we may use Theorem 4.3.5, since we also know that $E_i \subseteq LE_i \subseteq E_i(\zeta_{m_i})$ (recall we have proved Artin reciprocity for these cases).

Thus we have that:

$$\mathfrak{C}_{E_i} = (\alpha_{E_i})N_{LE_i/E_i}(\mathfrak{C}_{LE_i}),$$

for some $\alpha_{E_i} \in P_{E_i,1}(m_i\mathfrak{m}\mathfrak{O}_{E_i})$ and some $\mathfrak{C}_{LE_i} \in I_{LE_i}(m_i\mathfrak{m})$.

Then we can write:

$$\mathfrak{p}_i^{\gamma_i}(N_{E/K}(\mathfrak{b}))^{-d_i} = N_{E_i/K}(\mathfrak{C}_{E_i}) = N_{E_i/K}((\alpha_{E_i})N_{LE_i/E_i}(\mathfrak{C}_{LE_i})) = (N_{E_i/K}(\alpha_{E_i}))N_{LE_i/K}(\mathfrak{C}_{LE_i}).$$

But the term on the extreme right is in $P_{K,1}(m_i\mathfrak{m})N_{L/K}(I_L(m_i\mathfrak{m}))$ (this is easy to check by the properties of α_{E_i} and $\mathfrak{C}_{LE_i}$).

Finally, after taking the product over all i we see that:

$$\prod_{i=1}^{r} \mathfrak{p}_i^{\gamma_i}(N_{E/K}(\mathfrak{b}))^{-d_i} = \mathfrak{a}(N_{E/K}(\mathfrak{b}))^{-d_1-d_2-\ldots-d_r} \in P_{K,1}(\mathfrak{m})N_{L/K}(\mathfrak{m}).$$

Earlier we saw that $(-d_1 - d_2 - \ldots - d_r)$ is divisible by $n = [L : K]$, so that $(-d_1 - d_2 - \ldots - d_r) = -dn$ for some integer d. Then:

$$\mathfrak{a}(N_{E/K}(\mathfrak{b}))^{-d_1-d_2-\ldots-d_r} = \mathfrak{a}(N_{E/K}(\mathfrak{b})^{-d})^n = \mathfrak{a}N_{L/K}(N_{E/K}(\mathfrak{b})^{-d}\mathfrak{O}_L),$$

is in $P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$.

But:

$$N_{L/K}(N_{E/K}(\mathfrak{b})^{-d}\mathfrak{O}_L) \in P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$$

since $N_{E/K}(\mathfrak{b}) \in I_K(\mathfrak{m})$. It now follows that $\mathfrak{a} \in P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$ and so we are done.

□

Now that the hard work has been done, we deduce the case for Abelian extensions as a corollary.

Corollary 4.3.13. *Let L/K be a finite Abelian extension of number fields. Then there exists a complete modulus $\mathfrak{m}$ of L/K such that $\ker(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$ (i.e. $P_{K,1}(\mathfrak{m}) \subseteq \ker(\Phi_{L/K,\mathfrak{m}})$ for some complete modulus $\mathfrak{m}$ of K.*

Proof. We know that for each cyclic extension E/K with $K \subseteq E \subseteq L$ there exists some complete modulus $\mathfrak{m}_E$ of E/K such that $P_{K,1}(\mathfrak{m}_E) \subseteq \ker(\Phi_{E/K,\mathfrak{m}_E})$.

Define $\mathfrak{m} = \prod_E \mathfrak{m}_E$, so that $P_{K,1}(\mathfrak{m}) \subseteq P_{K,1}(\mathfrak{m}_E)$ for all such E. This tells us that $P_{K,1}(\mathfrak{m})$ is in the Artin kernel $\ker(\Phi_{E/K,\mathfrak{m}_E})$ for all such E. We need to show that this information is enough to let us conclude that $P_{K,1}(\mathfrak{m})$ actually lies in $\ker(\Phi_{L/K,\mathfrak{m}})$.

Take $\mathfrak{a} \in P_{K,1}(\mathfrak{m})$. By the above we must have that $\left(\frac{E/K}{\mathfrak{a}}\right) = 1$ for all such cyclic E/K. By restriction properties we thus see that:

$$\left(\frac{L/K}{\mathfrak{a}}\right)\Big|_E = 1,$$

for every E. We show that $\left(\frac{L/K}{\mathfrak{a}}\right) = 1$ and then we will be done.

Suppose not and let G' be the cyclic subgroup of $\mathrm{Gal}(L/K)$ generated by $\left(\frac{L/K}{\mathfrak{a}}\right)$. If $\left(\frac{L/K}{\mathfrak{a}}\right) \neq 1$ then G' is a non-trivial group and so there exists a non-trivial character:

$$\chi : G' \longrightarrow \mathbb{C}^\times.$$

Specifically, we must have that $\chi\left(\left(\frac{L/K}{\mathfrak{a}}\right)\right) \neq 1$.

We can extend χ to give a non-trivial character of $\mathrm{Gal}(L/K)$ (which we also denote as χ) and consider $H = \ker(\chi)$.

Now the image of χ is a finite group lying inside $\mathbb{C}^\times$ and so is a cyclic group. By the first isomorphism theorem we then have that $\mathrm{Gal}(L/K)/H$ is cyclic.

Taking E to be the fixed field of H we see that $\mathrm{Gal}(E/K)$ must also be cyclic (it is isomorphic to the quotient $\mathrm{Gal}(L/K)/H$ by the Galois correspondence). Thus this particular E/K is a cyclic extension.

But now we know that $\left(\frac{L/K}{\mathfrak{a}}\right)\Big|_E = 1$ and so $\left(\frac{L/K}{\mathfrak{a}}\right) \in H$, meaning that $\chi\left(\left(\frac{L/K}{\mathfrak{a}}\right)\right) = 1$, which is a contradiction.

Thus we must have that $\left(\frac{L/K}{\mathfrak{a}}\right) = 1$ and so $\mathfrak{a} \in \ker(\Phi_{L/K,\mathfrak{m}})$ which is what was required. □

So that is it, Artin reciprocity is proved. It took a lot of hard work but in wading through we have uncovered lots of interesting maths. We now move on to proving the second of the two main theorems, the existence theorem.

4.4 Proving the existence theorem

The proof of the existence theorem is all that remains for us to be able to finish proving the main theorems of class field theory. In order to prove it we need a notion of Artin map for ideles. After this we can restate the existence theorem in a new form, using the notion of a class field for a given open subgroup H with $K^\times \subseteq H \subseteq J_K$. Unfortunately due to page limitations certain longer proofs will be referenced.

Let L/K be an Abelian extension of number fields. The idelic Artin map on L/K works as follows. Choose a modulus $\mathfrak{m}$ of K such that $K^\times N_{L/K}(J_L) \supseteq E_{K,\mathfrak{m}}$ (such a modulus exists by Corollary 4.2.2).

For this modulus we have by earlier results that:

$$J_K/K^\times N_{L/K}(J_L) \cong I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m})).$$

But also by Artin reciprocity we know that:

$$I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m})) \cong \mathrm{Gal}(L/K).$$

Finally we have the canonical surjective homomorphism:

$$J_K \longrightarrow J_K/K^\times N_{L/K}(J_L),$$

given by $\mathbf{a} \longmapsto \mathbf{a} + K^\times N_{L/K}(J_L)$.

Putting all of this together, by composition we see that we have a surjective homomorphism:

$$\rho_{L/K} : J_K \longrightarrow \mathrm{Gal}(L/K).$$

This is the Artin map for ideles. We sometimes denote $\rho_{L/K}(\mathbf{a})$ by $\left(\frac{L/K}{\mathbf{a}}\right)$ to keep the notation consistent with the Artin map for ideals. The kernel of the idelic Artin map is $K^\times N_{L/K}(J_L)$ (since this is the kernel of the surjection onto $J_K/K^\times N_{L/K}(J_L)$ mentioned above).

Let $\mathfrak{m}$ be a modulus of K. Note that the idea of congruence subgroup for $\mathfrak{m}$ in the idele theory is exactly the same as subgroups of J_K containing $K^\times E_{K,\mathfrak{m}}$ in the idele theory (by one of the isomorphisms above). But we know from earlier that such an idele subgroup is the same as an open subgroup of J_K containing $K^\times$ (we had a one-to-one correspondence between the two things).

This means that we can define the following:

Definition 4.4.1. Let K be a number field and let H be an open subgroup of J_K containing $K^\times$. We say that H has a *class field* L (over K) if L/K is an Abelian extension of number fields and $H = K^\times N_{L/K}(J_L)$.

By Artin reciprocity, this is the same as saying that $H = \ker(\rho_{L/K})$. Also, note that such a group H has finite index in J_K. To see this recall that earlier we showed that:

$$J_K/K^\times E_{K,\mathfrak{m}} \cong I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m})),$$

the right hand side being a finite group. Thus $J_K/K^\times E_{K,\mathfrak{m}}$ is a finite group and the fact that $H \supseteq K^\times E_{K,\mathfrak{m}}$ tells us that J_K/H must be finite.

Now that we have this definition we can rewrite the statement of the existence theorem in the idelic form.

Theorem 4.4.2. *(Existence theorem) Let K be a number field and H be an open subgroup of J_K containing $K^\times$. Then H has a class field over K for some Abelian extension L/K of number fields.*

Actually, once this is proved it will follow that the class field over K of such a H is unique. To see this consider:

$$E = \{\text{number fields } L \text{ containing } K \mid L/K \text{ is Abelian}\}$$

and:

$$F = \{\text{open subgroups } H \text{ of } J_K \mid H \text{ contains } K^\times\}$$

We will have a bijection:

$$\Phi : E \longrightarrow F,$$

given by $\Phi(L) = K^\times N_{L/K}(J_L)$. Injectivity will follow by Artin reciprocity and surjectivity will follow by the existence theorem. Thus the class field will be unique by this one-to-one correspondence.

In order to prove the existence theorem we need a few nice results about class fields. After a brief discussion we will reduce the situation to the case where K contains a certain group of nth roots of unity. This will lead nicely into the study of Kummer n-extensions.

Lemma 4.4.3. *Let H and H' be open subgroups of J_K containing $K^\times$. If H has class field L over K and $H \subseteq H'$ then H' has a class field over K.*

Proof. We have the Artin map $\rho_{L/K}$ and we know that $H = \ker(\rho_{L/K})$ by definition of class field. Consider the subgroup $\rho_{L/K}(H')$ of $\mathrm{Gal}(L/K)$ and define the field L' to be the fixed field of $\rho_{L/K}(H')$ (it is a subgroup of $\mathrm{Gal}(L/K)$, since it the image of the Artin map homomorphism). We show that L' is a class field for H' over K.

By the order reversing property of the Galois correspondence we must have that $K \subseteq L' \subseteq L$ (since $H \subseteq H'$ so that $\rho_{L/K}(H) \subseteq \rho_{L/K}(H')$ as subgroups of $\mathrm{Gal}(L/K)$). We must show that $H' = \ker(\rho_{L'/K})$.

In the same way as ideals the idelic Artin symbol also satisfies the restriction property:

$$\left(\frac{L/K}{\mathbf{a}}\right)\Big|_{L'} = \left(\frac{L'/K}{\mathbf{a}}\right).$$

Thus we have that $\mathbf{a} \in \ker(\rho_{L'/K})$ if and only if $\left(\frac{L/K}{\mathbf{a}}\right)\Big|_{L'} = 1$. But L' is the fixed field of $\rho_{L/K}(H')$ thus $\left(\frac{L/K}{\mathbf{a}}\right)\Big|_{L'} = 1$ if and only if $\left(\frac{L/K}{\mathbf{a}}\right) \in \rho_{L/K}(H')$.

Now $\rho_{L/K}(H')$ is a group and so we see that $\left(\frac{L/K}{\mathbf{a}}\right) \in \rho_{L/K}(H')$ if and only if there is some $\mathbf{b} \in H'$ such that $\left(\frac{L/K}{\mathbf{ab^{-1}}}\right) = 1$ (in other words the Artin symbol of $\mathbf{a}$ in L/K has an inverse Artin symbol for some $\mathbf{b} \in H'$). This is clearly equivalent to $\mathbf{ab^{-1}} \in \ker(\rho_{L/K}) = H$.

But we are done since this is the same as $\mathbf{a} \in HH' = H'$ (recall that $H \subseteq H'$). Thus we have that $\mathbf{a} \in \ker(\rho_{L'/K})$ if and only if $\mathbf{a} \in H'$, meaning that $H' = \ker(\rho_{L'/K})$ and so L' is a class field for H' over K. □

The next result will be very important. It will link class fields of preimage norms of H to class fields of H.

Theorem 4.4.4. *Let L/K be a cyclic extension of number fields and let H be an open subgroup of J_K containing $K^\times$. Define $H_L = N_{L/K}^{-1}(H) = \{\mathbf{x} \in J_L \mid N_{L/K}(\mathbf{x}) \in H\}$. If H_L has a class field over L then H has a class field over K.*

Proof. Let E be the class field of H_L over L. By definition, we have that $\mathrm{Gal}(E/L)$ is Abelian and that $H_L = L^\times N_{E/L}(J_E) = \ker(\rho_{E/L})$. Also, by definition we have that $N_{L/K}(H_L) = H$.

We omit the proof of the facts that E/K is a Galois extension and that it is Abelian. Given these facts and the definition of class field we know that the subgroup $K^\times N_{E/K}(J_L)$ of J_K has class field E over K.

The chain of inclusions:

$$K^\times N_{E/K}(J_L) \subseteq K^\times N_{L/K}(N_{E/L}(J_E)) \subseteq K^\times N_{L/K}(H_L) \subseteq K^\times H = H,$$

along with the previous result tells us that H has a class field over K (in fact by the proof of the previous result, a class field can be taken to be the fixed field of $\rho_{E/K}(H)$). □

Now we make the promised simplification. First we pause to make a simple definition:

Definition 4.4.5. An Abelian group G is said to have *exponent* n if $g^n = e$ for all $g \in G$.

Let H be an open subgroup of J_K containing $K^\times$. The group J_K/H has some finite exponent n (the group itself is finite so has to have some finite exponent less than or equal to the order of the group). Proving the existence theorem requires us to show that H has a class field over K.

If we adjoin a primitive nth root of unity ζ_n to K we can make the field extension $K(\zeta_n)/K$ (this is an Abelian extension of number fields).

By the theory of field extensions we can construct a tower of fields:

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_t = K(\zeta_n),$$

such that each extension K_i/K_{i-1} is cyclic. Define for each i the subgroups $H_i = N^{-1}_{K_i/K}(H)$ of J_{K_i} (these are the groups of preimage norms up to each level of the tower).

It can easily be shown using the fact that norms are multiplicative in towers that $H_i = N^{-1}_{K_i/K_{i-1}}(H_{i-1})$ for all i. Using the previous result, if we could show that H_t has a class field over $K_t = K(\zeta_n)$ then H_{t-1} would automatically have a class field over K_{t-1}. Then it would follow that H_{t-2} would have to have a class field over K_{t-2} and so on all the way down until we find out that $H_0 = H$ must have a class field over $K_0 = K$ (which is what we want to prove).

Considering this we only need to prove the existence theorem in the case where the number field is of the form $K(\zeta_n)$. Alternatively, we may assume that we are working in the case where K contains all of the nth roots of unity.

We make the following definition motivated by the above:

Definition 4.4.6. Let n be a positive integer. A finite Abelian extension L/K is called a *Kummer n-extension* if $\mathrm{Gal}(L/K)$ has exponent n and K contains all of the nth roots of unity.

From now on in this subsection we assume that K contains all nth roots of unity for some n (some of the results to follow do not apply to general number fields). The following nice result classifies all Kummer n-extensions of such a K (for this same n):

Theorem 4.4.7. *There is a one-to-one correspondence between the Kummer n-extensions of K and the finite subgroups of $K^\times/(K^\times)^n$. The correspondence is such that a given finite subgroup $W/(K^\times)^n$ gives rise to a Kummer n-extension $K(W^{\frac{1}{n}})/K$ with $\mathrm{Gal}(K(W^{\frac{1}{n}})/K) \cong W/(K^\times)^n$ (where $K(W^{\frac{1}{n}})$ denotes the extension of K formed by adjoining the nth roots of elements of W).*

Proof. See p.139-p.141 of [2]. The isomorphism:

$$\mathrm{Gal}(K(W^{\frac{1}{n}})/K) \cong W/(K^\times)^n,$$

is not a natural one. It depends on a choice of nth root of unity $\zeta \in K$ since for a given $\sigma \in \mathrm{Gal}(K(W^{\frac{1}{n}})/K)$ we have that $\sigma(a_i^{\frac{1}{n}}) = \zeta a_i^{\frac{1}{n}}$ (with $a_i \in W$). □

We now find more special subgroups of the ideles that will help us in our journey:

Definition 4.4.8. Let S be a finite set of places of K contining the infinite places of K. Define the *S-ideles* of J_K to be the subgroup:

$$J_{K,S} = \prod_{v \in S} K_v^\times \prod_{v \notin S} U_v.$$

Also define the *S-units* to be the subgroup:

$$K_S = J_{K,S} \cap K^\times,$$

where as usual we identify $K^\times$ with its embedding into J_K.

The fact that S is a finite set really does guarantee that these things are subgroups of the ideles. We immediately get a nice result about K_S:

Theorem 4.4.9. *Let S be as above and suppose that K contains all nth roots of unity (for some n). Then $[K_S : (K_S)^n] = n^{|S|}$.*

Proof. When K is any number field (not necessarily containing all nth roots of unity) we have that:

$$K_S \cong W_K \times \mathbb{Z}^{|S|-1},$$

where W_K is the group of nth roots of unity that lie in K. The proof of this claim can be found on p.142 of [2] and uses Dirichlet's unit theorem.

From this we can see that when K contains all nth roots of unity we must have that $W_K = \langle \zeta_n \rangle$. We then perform the quotient and see that:

$$K_S/(K_S)^n \cong \langle \zeta_n \rangle / \langle \zeta_n \rangle^n \times \mathbb{Z}^{|S|-1}/n(\mathbb{Z}^{|S|-1}) \cong \langle \zeta_n \rangle / \langle \zeta_n \rangle^n \times (\mathbb{Z}/n\mathbb{Z})^{|S|-1}.$$

The first group has order n and the second has order $n^{|S|-1}$. Thus $[K_S : (K_S)^n] = n^{|S|}$. □

This result has local analogues:

Lemma 4.4.10. *Let v be a finite place of K (recall we assume that K contains all nth roots of unity for some n). Then:*

$$[U_v : (U_v)^n] = \frac{n}{|n|_v}$$

$$[K_v^\times : (K_v^\times)^n] = \frac{n^2}{|n|_v}.$$

Proof. See p.143-p.144 of [2]. Intuitively, the result seems likely to hold since we would expect both indices to have a some kind of connection with n. Dividing by $|n|_v$ essentially accounts for the fact that the index might be bigger than n when $\mathrm{ord}_v(n) \geq 1$ due to ramification (recall that $|n|_v \leq 1$ under all finite places v since n is an integer). □

We now reach a point where we can prove the existence theorem. We do this indirectly. First we need the following result that lets us rewrite J_K interms of the S-ideles for some S:

Lemma 4.4.11. *We can write $J_K = K^\times J_{K,S}$ for some finite set of places S of K containing the infinite ones.*

Proof. Consider representatives $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_{h_K}$ for the ideal classes in the ideal class group of K (the ideal class group is finite so we can take finitely many representatives). Factorise each of these representatives into prime ideals and consider the entire list $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m$. Take S to be the set of places consisting of all infinite places of K and all finite places of K corresponding to these prime ideals. We show that the result holds for this S.

Firstly it is clear that $K^\times J_{K,S} \subseteq J_K$, since both $K^\times$ and $J_{K,S}$ are subgroups of J_K. We show the reverse inclusion.

Take $\mathbf{a} \in J_K$ and write $\mathbf{a} = (\ldots, a_v, \ldots)$. Now apply the map η from the proof of Proposition 3.1.4 to get:

$$\eta(\mathbf{a}) = \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v(a_v)}.$$

By the fact that $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_{h_K}$ form representatives for the ideal class group of K we must have that $\eta(\mathbf{a}) \in \mathfrak{a}_i P_K$ for some i. Thus $\eta(\mathbf{a}) = (\alpha)\mathfrak{a}_i$ for some $\alpha \in K^\times$.

This then tells us that $\eta(\alpha^{-1}\mathbf{a}) = \mathfrak{a}_i$ so that:

$$\prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v(\alpha^{-1}a_v)} = \mathfrak{a}_i.$$

But the only prime ideal factors of $\mathfrak{a}_i$ are in the list $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m$ and these corresponded to places in S, so we must have that $\mathrm{ord}_v(\alpha^{-1}\mathbf{a}) = 0$ for all $v \notin S$. Thus $\alpha^{-1}\mathbf{a} \in J_{K,S}$ which gives $\mathbf{a} \in K^\times J_{K,S}$. □

It should be clear that if S is such that the above result is true, then extending to another finite set of places $S' \supseteq S$ will still give us the equality $J_K = K^\times J_{K,S'}$.

We now exhibit a special subgroup of the S-ideles that has a class field over K (when S is a special set of places).

Theorem 4.4.12. *Let K be a number field that contains all of the nth roots of unity for some n. Construct a finite set of places S of K containing all infinite places of K, all finite places v such that $\mathfrak{p}_v | n\mathfrak{O}_K$ and enough extra finite places so that it is possible to write $J_K = K^\times J_{K,S}$.*

Then:

$$B = \prod_{v \in S} (K_v^\times)^n \prod_{v \notin S} U_v$$

is such that $K^\times B$ has a class field over K. Further, a class field can be taken to be $K((K_S)^{\frac{1}{n}})$ (which is the field K with the nth roots of K_S adjoined).

Proof. We start by realising that $K_S \cap (K^\times)^n = K_S^n$. Then, by use of the second isomorphism theorem we see that:

$$K_S(K^\times)^n/(K^\times)^n \cong K_S/(K_S \cap (K^\times)^n) = K_S/K_S^n.$$

But we have the equality $[K_S : (K_S)^n] = n^{|S|}$, telling us that $K_S(K^\times)^n/(K^\times)^n$ is a finite subgroup of $K^\times/(K^\times)^n$. This means that there is a corresponding Kummer n-extension L/K with $L = K(K_S^{\frac{1}{n}})$ and that the isomorphism $K_S(K^\times)^n/(K^\times)^n \cong \mathrm{Gal}(L/K)$ holds (this was an earlier result). It remains to show that $K^\times B = K^\times N_{L/K}(J_L)$ and then the result follows.

It is worth noting for the time being that for any $v \notin S$ we have that $\mathfrak{p}_v$ is unramified in L. To see this note that the generators of L over K are the solutions of equations $x^n - \alpha = 0$ for $\alpha \in K_S$. The formal derivative of $x^n - \alpha$ is nx^{n-1} and by the choice of S we have that $\mathfrak{p}_v$ does not divide n for any $v \notin S$. Thus the polynomial $x^n - \alpha$ has no repeated roots mod $\mathfrak{p}_v$ for any $v \notin S$ and so all such $\mathfrak{p}_v$ are unramified in L.

First we show the forwards inclusion $K^\times B \subseteq K^\times N_{L/K}(J_L)$. Now $\mathrm{Gal}(L/K)$ has exponent n so that given any $v \in S$ and $x \in (K_v^\times)^n$ we have that the idele $(\ldots, x, \ldots)$ lies inside $\ker(\rho_{L/K}) = K^\times N_{L/K}(J_L)$ (where the x appears in the component corresponding to the place v).

Thus:

$$\prod_{v \in S} (K_v^\times)^n \subseteq K^\times N_{L/K}(J_L).$$

Whenever $v \notin S$, we find that for any $x \in U_v$ there is some $y \in U_w$ such that $x = N_{L_w/K_v}(y)$ (where w is a place of L lying above v). This is a consequence of earlier results since each $v \notin S$ is unramified and so $[U_v : N_{L_w/K_v}(U_v)] = 1$ for each place w of L lying above v, leading to the equality $U_v = N_{L_w/K_v}(U_w)$.

So we must have that:

$$\prod_{v \notin S} U_v \subseteq N_{L/K}(J_L).$$

Thus $K^\times B \subseteq K^\times N_{L/K}(J_L)$ (we have checked that the two products defining B lie in the required group).

Instead of proving the reverse inclusion we note the following:

$$[J_K : K^\times N_{L/K}(J_L)] = |\mathrm{Gal}(L/K)| = n^{|S|}.$$

To see this we use Artin reciprocity for the first equality and the discussion at the start of the proof for the second equality. If we can show that $[J_K : K^\times B] = n^{|S|}$, then this and the inclusion $K^\times B \subseteq K^\times N_{L/K}(J_L)$ will imply that $K^\times B = K^\times N_{L/K}(J_L)$, which is the equality we want.

By our choice of S we may write:

$$[J_K : K^\times B] = [K^\times J_{K,S} : K^\times B].$$

Then we can use both the third and second isomorphism theorems (in that order) to see that:

$$[K^\times J_{K,S} : K^\times B] = \frac{[J_{K,S} : B]}{[J_{K,S} \cap K^\times : B \cap K^\times]} = \frac{[J_{K,S} : B]}{[K_S : B \cap K^\times]}.$$

But the quotient group $J_{K,S}/B$ is isomorphic to:

$$\prod_{v\in S} K_v^\times/(K_v^\times)^n,$$

since for all $v \notin S$ the corresponding components of both $J_{K,S}$ and B are the same unit group U_v.

So we now have that:

$$\frac{[J_{K,S}:B]}{[K_S:B\cap K^\times]} = \frac{\prod_{v\in S}[K_v^\times:(K_v^\times)^n]}{[K_S:B\cap K^\times]} = \frac{\prod_{v\in S}\frac{n^2}{|n|_v}}{[K_S:B\cap K^\times]} = \frac{n^{2|S|}}{[K_S:B\cap K^\times]},$$

where the last equality follows from the product formula for absolute values.

We finally show that $B\cap K^\times = (K_S)^n$, since then it will follow that:

$$\frac{n^{2|S|}}{[K_S:B\cap K^\times]} = \frac{n^{2|S|}}{[K_S:(K_S)^n]} = \frac{n^{2|S|}}{n^{|S|}} = n^{|S|},$$

which will tell us that $[J_K : K^\times B] = n^{|S|}$ (this is what we want).

The inclusion $(K_S)^n \subseteq B\cap K^\times$ is trivial. To get the other inclusion take $x \in B\cap K^\times$. By the definition of B we now see that x can be realised for each $v \in S$ as an nth power in $K_v^\times$. But then we find that $x^{\frac{1}{n}} \in K_v^\times$ and so the extension $K_v(x^{\frac{1}{n}})/K_v$ has degree 1. Thus $\mathfrak{p}_v$ splits completely in $K(x^{\frac{1}{n}})/K$ for each $v \in S$ (because the Galois group of the extension $K_v(x^{\frac{1}{n}})/K_v$ is trivial so that the Artin symbol must be trivial). When $v \notin S$ we know that $\mathfrak{p}_v$ is unramified in $K(x^{\frac{1}{n}})$.

Stringing the previous paragraph together, we have shown that $J_{K,S} \subseteq N_{K(x^{\frac{1}{n}})/K}\left(J_{K(x^{\frac{1}{n}})}\right)$ and since $J_K = K^\times J_{K,S}$ we see that:

$$J_K \subseteq K^\times N_{K(x^{\frac{1}{n}})/K}\left(J_{K(x^{\frac{1}{n}})}\right) = \ker\left(\rho_{K(x^{\frac{1}{n}})/K}\right).$$

But by definition of the Artin map we know that:

$$\ker\left(\rho_{K(x^{\frac{1}{n}})/K}\right) \subseteq J_K,$$

and so the Artin kernel with respect to the extension $K(x^{\frac{1}{n}})/K$ is the whole of J_K. This tells us that $\mathrm{Gal}(K(x^{\frac{1}{n}})/K)$ is trivial so that $x^{\frac{1}{n}} \in K$. But $x \in B$ and so $x \in K_S$ which is what we wanted. We are now done. □

After all of the hard work above, we now find that the existence theorem is a mere corollary.

Corollary 4.4.13. *(Existence theorem) Let K be a number field and H be an open subgroup of J_K that contains $K^\times$. Then H has a class field over K for some Abelian extension L/K of number fields.*

Proof. Let J_K/H have exponent n. As mentioned earlier we can assume that K contains the nth roots of unity. Take S to be the finite set of places in the above theorem. If we extend S to include the places v such that $U_v \not\subseteq H$ then we find that $B \subseteq H$.

But now we have that $H = K^\times H \supseteq K^\times B$ and we have just seen that for such an S we have that $K^\times B$ has a class field over K. Thus by Lemma 4.4.3, we must have that H has a class field over K. □

We are now done proving the two main theorems of class field theory. Finally the correspondence between Abelian extensions of number fields and generalised ideal class groups is apparent. We may now concern ourselves with a nice application of the ideas.

5 Primes of the form $x^2 + ny^2$

In this section we consider the question of which primes p can be written in the form $x^2 + ny^2$ for a fixed positive integer n.

Clearly the ring $\mathbb{Z}\left[\sqrt{-n}\right]$ is going to be helpful here by the factorisation:

$$x^2 + ny^2 = (x + y\sqrt{-n})(x - y\sqrt{-n}).$$

So we work with the imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$ in order to exploit this.

Unfortunately, we have to be careful since $\mathbb{Z}\left[\sqrt{-n}\right]$ is not always the ring of integers of such a number field (it all depends on the value of n mod 4). This means that we would not be able to assume that we have nice behaviour even in terms of factorisation of ideals (sometimes these rings are not Dedekind domains so factorisation into prime ideals might not be unique).

However, the question can be answered easily if we restrict our attention to square-free n such that $n \not\equiv 3 \bmod 4$. Here we do have that $\mathbb{Z}\left[\sqrt{-n}\right]$ is the ring of integers and so is automatically a Dedekind domain (so the problems above do not apply to us). In this section we provide the solution for these n and later we provide some examples and a brief discussion of the other cases.

5.1 A theoretical solution to the problem

Let K be any number field and consider the modulus $\mathfrak{m} = (1)$ of K. Then we have that $I_K(\mathfrak{m}) = I_K$ and $P_{K,1}(\mathfrak{m}) = P_K$.

Now P_K is itself a congruence subgroup for this $\mathfrak{m}$. Thus, the existence theorem guarantees the existence of a field K_H such that K_H/K is Abelian and:

$$I_K/P_K \cong \mathrm{Gal}(K_H/K),$$

the isomorphism being via the Artin map.

Further, the extension K_H/K is unramified at all places not dividing $\mathfrak{m}$ (so is unramified at all places of K since $\mathfrak{m}$ is trivial). By Galois theory, this is the maximal such extension with respect to inclusion of fields since P_K is the smallest possible congruence subgroup for $\mathfrak{m}$.

Definition 5.1.1. We call the field K_H the *Hilbert class field* of K.

Tying all of this together we find that the Hilbert class field is the maximal unramified Abelian extension of K. Any other Abelian extension of K that is unramified at all places of K must be contained inside this one. Also, the Galois group of the Galois extension K_H/K is isomorphic to the ideal class group of K so that the degree of the extension is the class number h_K.

This is remarkable in many ways. First, it is strange that there should be such a maximal extension and second, it is strange that there is a link with the ideal class group (a group that is just connected to the base field K). It is counter-intuitive that there should be any link between Abelian extensions of K and the arithmetic inside K. These points obviously echo throughout class field theory since the more general results show both of these characteristics too.

Also, if we drop the Abelian part we may ask if there always exists a maximal unramified extension of K. Unfortunately the answer is no. In fact, it was shown by Golod and Shafarevich that the imaginary quadratic field $\mathbb{Q}(\sqrt{-2.3.5.7.11.13})$ has unramified extensions of arbitrarily high degree.

The Hilbert class field was defined in the previous project but it was necessary to derive its existence again now that we have proved the main theorems of class field theory. Historically, the Hilbert class field was conjectured and proved to exist before class field theory was studied.

One amazing property of the Hilbert class field is the following:

Lemma 5.1.2. *Let K be a number field and let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$. Then $\mathfrak{p}$ splits completely in K_H if and only if $\mathfrak{p}$ is a principal ideal of $\mathfrak{O}_K$.*

Proof. This is not too difficult to prove. We know that $\mathfrak{p}$ splits completely in K_H if and only if the Artin symbol $\left(\frac{K_H/K}{\mathfrak{p}}\right)$ is trivial.

But under the isomorphism:

$$I_K/P_K \cong \mathrm{Gal}(K_H/K),$$

we see that this Artin symbol is trivial if and only if $\mathfrak{p}$ lies in the trivial class of I_K/P_K (i.e. the kernel of the Artin map). This is equivalent to saying that $\mathfrak{p} \in P_K$ which by definition is the same as $\mathfrak{p}$ being principal. □

There are many other nice properties of the Hilbert class field. One of them is the fact that when K has a principal ideal domain as its ring of integers then K is its own Hilbert class field (so that every other extension of K must have some ramification). This is easily seen because here the class number h_K is 1 so that $[K_H : K] = 1$, meaning that $K_H = K$. The field $\mathbb{Q}$ is an example of this.

Another is that for any ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ the ideal $\mathfrak{a}\mathfrak{O}_{K_H}$ is principal as an ideal of $\mathfrak{O}_{K_H}$. Essentially this result tells us that all ideals of $\mathfrak{O}_K$ become principal in $\mathfrak{O}_{K_H}$. This theorem is the *principal ideal theorem* and is not as easy to prove as it seems.

The principal ideal theorem does not imply that K_H is a principal ideal domain, only that ideals of $\mathfrak{O}_{K_H}$ lying above ideals of $\mathfrak{O}_K$ must be principal. In fact we can take the Hilbert class field of K_H and quite often this field is not the same as K_H. Doing this over and over again we can construct towers of Hilbert class fields and a popular question is whether these towers always terminate. This is the same thing as asking whether each number field can be extended finitely many times to give one with class number 1 (i.e. a field with unique factorisation into irreducibles).

Again the answer to this question was provided by Golod and Shafarevich. They supplied the quadratic field $\mathbb{Q}(\sqrt{3.7.11.13.19.23})$ as an example of a number field that has an infinite Hilbert class field tower. So this field cannot be embedded inside a finite extension field that has unique factorisation.

Now that we have discussed the properties of the Hilbert class field we are ready to tackle the problem posed at the start of this section. We do this in two stages.

For the rest of this subsection we assume that n is a square-free positive integer and that $n \not\equiv 3 \bmod 4$. Then the number field $K_n = \mathbb{Q}(\sqrt{-n})$ has ring of integers $\mathfrak{O}_{K_n} = \mathbb{Z}[\sqrt{-n}]$. We have the existence of the Hilbert class field K_{n_H} of K_n and we are able to apply the theory that we have discussed above.

First we relate being able to write $p = x^2 + ny^2$ to the way p splits in K_{n_H}.

Theorem 5.1.3. *Let n be as above and let p be a rational prime not dividing n. We have that:*

$$p = x^2 + ny^2 \iff p \text{ splits completely in } K_{n_H}.$$

Proof. We know that the discriminant of K_n is $d_{K_n} = -4n$. Now p is an odd prime not dividing n so p cannot divide $-4n$. This tells us that p is unramified in K (because p does not divide d_{K_n}).

First we prove that:

$$p = x^2 + ny^2 \iff p\mathfrak{O}_{K_n} = \mathfrak{p}\bar{\mathfrak{p}},$$

where $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are distinct principal prime ideals of $\mathfrak{O}_{K_n}$ generated by conjugates $\alpha, \bar{\alpha} \in \mathfrak{O}_{K_n}$. This is not too difficult to see, for if $p = x^2 + ny^2$ then $p = (x + y\sqrt{-n})(x - y\sqrt{-n})$. When we move to ideals we get $p\mathfrak{O}_{K_n} = \mathfrak{p}\bar{\mathfrak{p}}$ with $\mathfrak{p} = (x + y\sqrt{-n})\mathfrak{O}_{K_n}$ and $\bar{\mathfrak{p}} = (x - y\sqrt{-n})\mathfrak{O}_{K_n}$.

These two ideals must be distinct since p is unramified in K and they must be prime by the uniqueness of prime ideal factorisation in $\mathfrak{O}_{K_n}$ (since $p\mathfrak{O}_{K_n}$ has already split into two ideals in the imaginary quadratic field K_n). Both of these ideals are principal and are generated by elements of $\mathfrak{O}_{K_n}$.

Conversely, if $p\mathfrak{O}_{K_n} = \mathfrak{p}\bar{\mathfrak{p}}$ for two distinct principal prime ideals $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ of $\mathfrak{O}_{K_n}$ then $\mathfrak{p} = (x+y\sqrt{-n})\mathfrak{O}_{K_n}$ and $\bar{\mathfrak{p}} = (x-y\sqrt{-n})\mathfrak{O}_{K_n}$. Thus $p\mathfrak{O}_{K_n} = (x^2+ny^2)\mathfrak{O}_{K_n}$ so that p and x^2+ny^2 are associates in $\mathfrak{O}_{K_n}$. It can easily be checked that in either case we may take $p = x^2 + ny^2$ (we are working in an imaginary quadratic field so there are finitely many units and they are known, see p.77 of [7]). Thus the equivalence above is shown.

We know that $p\mathfrak{O}_{K_n} = \mathfrak{p}\bar{\mathfrak{p}}$ for two distinct prime ideals $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ of $\mathfrak{O}_{K_n}$ if and only if p splits completely in K_n (this is because we are working in a quadratic field). Also, by Lemma 5.1.2 we know that $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are

principal prime ideals if and only if $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ split completely in K_{n_H}. These two facts together tell us that (for two distinct *principal* prime ideals $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ of $\mathfrak{O}_{K_n}$):

$$p\mathfrak{O}_{K_n} = \mathfrak{p}\bar{\mathfrak{p}} \iff p \text{ splits completely in } K_n \quad \text{and} \quad \mathfrak{p}, \bar{\mathfrak{p}} \text{ split completely in } K_{n,H}.$$

Since ramification indices work in towers we see that the right hand side of the above is equivalent to p splitting completely in K_{n_H} as required. □

The next implication connects the splitting of p in K_H to congruence conditions mod p.

Theorem 5.1.4. *Let K be an imaginary quadratic field. We have that:*

1. *there is a real algebraic integer α such that $K_H = K(\alpha)$;*
2. *if $f(x) \in \mathbb{Z}[x]$ is the minimal polynomial of α over $\mathbb{Q}$ and p is a prime not dividing the discriminant of $f(x)$ then:*

$$p \text{ splits completely in } K_H \iff \left(\frac{d_K}{p}\right) = 1 \quad \text{and} \quad f(a) \equiv 0 \bmod p \quad \text{for some } a \in \mathbb{Z}.$$

Proof. Firstly, we must have complex conjugation τ as an automorphism of $\mathrm{Gal}(K_H/K)$. To see this, note that $\tau(K_H)$ is an unramified extension of $\tau(K) = K$. Thus $\tau(K_H) \subseteq K_H$ by maximality of K_H. Also, $\tau(K_H)/K$ has the same degree as K_H/K so that $\tau(K_H) = K_H$. Using this and the fact that K is imaginary quadratic it can be shown that $K_H/\mathbb{Q}$ must be Galois.

The fixed field of complex conjugation here is the field $K_H \cap \mathbb{R}$ and by Galois theory we have to have that $[K_H \cap \mathbb{R} : \mathbb{Q}] = [K_H : K]$. It is easily shown that given an element $\alpha \in K_H \cap \mathbb{R}$ such that $K_H \cap \mathbb{R} = \mathbb{Q}(\alpha)$ then this α is such that $K_H = K(\alpha)$. The converse is also true (in other words real generators for one of the two extensions immediately work for the other extension).

Choosing such a generator $\alpha \in \mathfrak{O}_{K_H} \cap \mathbb{R}$ (this can be done by properties of algebraic integers) we find that the first claim is proved. Also by the equality of the degrees above we find that the minimal polynomial $f(x)$ of such an α over $\mathbb{Q}$ must be the same as the minimal polynomial of α over K.

To prove the second claim suppose p is a prime number that does not divide the discriminant of $f(x)$. Then $f(x)$ is separable mod p. But we are working in a quadratic number field so we have a factorisation:

$$p\mathfrak{O}_K = \mathfrak{p}\bar{\mathfrak{p}},$$

where $\mathfrak{p} \neq \bar{\mathfrak{p}}$. By the theory of splitting of primes in quadratic fields, this happens if and only if $\left(\frac{d_K}{p}\right) = 1$.

We can assume that p splits in K. Then $\mathbb{Z}/p\mathbb{Z} \cong \mathfrak{O}_K/\mathfrak{p}$ and $f(x)$ is separable mod p (where $\mathfrak{p}$ is one of the prime ideal factors of $p\mathfrak{O}_K$). This means that $f(x)$ is separable in $\mathfrak{O}_K/\mathfrak{p}$ too. But we know that $\mathfrak{p}$ splits completely in K_H if and only if $f(x) \equiv 0 \bmod \mathfrak{p}$ has a solution in $\mathfrak{O}_K$ (this is a well known result in algebraic number theory, see p.102 of [3]). But by the above this congruence is satisfied if and only if $f(x) \cong 0 \bmod p$ has a solution in $\mathbb{Z}$. This proves the second claim. □

Note that by field theory and the isomorphisms from earlier, the polynomial $f(x)$ will have to have degree $[K_H : K] = h_K$. Putting the previous two theorems together gives us the following:

Corollary 5.1.5. *Let n be a positive integer. Then there is a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree h_{K_n} such that if an odd prime p divides neither n nor the discriminant of $f_n(x)$, then:*

$$p = x^2 + ny^2 \iff \left(\frac{-n}{p}\right) = 1 \quad \text{and} \quad f_n(a) \equiv 0 \bmod p \quad \text{for some } a \in \mathbb{Z}.$$

Further, the polynomial $f_n(x)$ can be taken to be the minimal polynomial of over $\mathbb{Z}$ of any real algebraic integer that generates K_{n_H}, the Hilbert class field of K_n.

Proof. Most of this follows directly from the previous two theorems by taking $K = K_n$. Take a real algebraic integer α such that $K_H = K(\alpha)$. Then the minimal polynomial of α must have degree h_{K_n} since $[K_H : K] = h_{K_n}$. It just remains to prove the Legendre symbol claim. Note that $d_{K_n} = -4n$ and so the Legendre symbol $\left(\frac{d_K}{p}\right)$ is the same as $\left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right)$ by multiplicativity of the Legendre symbol. □

Since the generator of a field extension is not unique the polynomial $f_n(x)$ will not be unique but actually this does not matter here, they will all give the same congruence conditions when considered mod p.

This completes our partial solution of the problem although in general Hilbert class fields are quite hard to find explicitly. This is why our solution is only theoretical. In order for us to solve the problem practically for the n we have considered, we would need a method for computing the Hilbert class field for any imaginary quadratic field. Fortunately this problem has been solved using j-invariants of elliptic curves and modular forms. The computational solution is far beyond the scope of this project but an interested reader can read Chapter 3 of [3].

5.2 Three examples

We finish off the project by applying the theory to a few easier cases. We first consider the case $n = 14$ in detail. We follow [3] with this example and find the Hilbert class field explicitly. Then we provide a solution of the case $n = 21$ making use of tables in [4]. Finally we make a brief discussion of the solution of this problem for general n and provide the example $n = 27$ to motivate this.

Let us start with the case $n = 14$. Here we use the imaginary quadratic field $K_{14} = \mathbb{Q}(\sqrt{-14})$. The discriminant of K_{14} is $4 \times (-14) = -56$ and the ring of integers of K_{14} is $\mathfrak{O}_{K_{14}} = \mathbb{Z}[\sqrt{-14}]$, both as expected ($n$ satisfies the conditions mentioned earlier). By direct computation or by use of class number tables we find that the class number of K_{14} is 4. This tells us that the Hilbert class field K_{14_H} is of degree 4 over K_{14}. The claim is that $K_{14_H} = K_{14}(\sqrt{2\sqrt{2}-1})$.

First we need a small lemma about ramification in certain quadratic extensions.

Lemma 5.2.1. *Let $L = K(\sqrt{u})$ for some $u \in \mathfrak{O}_K$ be a quadratic extension and let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_K$. We have that:*

1. *if $2u \notin \mathfrak{p}$ then $\mathfrak{p}$ is unramified in L;*
2. *if $2 \in \mathfrak{p}$, $u \notin \mathfrak{p}$ and $u = b^2 - 4c$ for some $b, c \in \mathfrak{O}_K$ then $\mathfrak{p}$ is unramified in L.*

Proof. For the first claim note that $\sqrt{u} \notin K$, since we are assuming $K(\sqrt{u})$ to be a quadratic extension of K. Thus $\sqrt{u}$ has minimal polynomial $x^2 - u$ over K. This has discriminant $4u \notin \mathfrak{p}$ and so we see that $x^2 - u$ factors into linear polynomials mod $\mathfrak{p}$. Thus $\mathfrak{p}$ is unramified in K (using the connection between factorisation of primes in extension fields and solutions of the minimal polynomial mod $\mathfrak{p}$).

For the second claim we can rewrite L as $K(\frac{-b+\sqrt{u}}{2})$. This generator has minimal polynomial $x^2 + bx + c$ over K. The discriminant of this quadratic is $b^2 - 4c \notin \mathfrak{p}$ and so similarly to the first claim the polynomial must factor into linear polynomials mod $\mathfrak{p}$. Thus $\mathfrak{p}$ is unramified in K. □

This unusual lemma is needed to prove our claim.

Lemma 5.2.2. *The Hilbert class field of $K_{14} = \mathbb{Q}(\sqrt{-14})$ is $L = K_{14}\left(\sqrt{2\sqrt{2}-1}\right)$.*

Proof. We show that L/K_{14} is an unramified Abelian extension of degree 4. Then it will follow by uniqueness of the Hilbert class field that L must be the right one (there can be more than one primitive element for an extension field, it is the field itself that is unique).

It is already clear that L/K_{14} is an Abelian extension of degree 4. The degree is easily verified and recall that all groups of order 4 are Abelian so that the Abelian nature of the extension is trivial. It remains to show that L/K_{14} is unramified.

Since K_{14} is imaginary quadratic there are no real embeddings of K_{14} and so we only need to check that all finite places of K_{14} are unramified in L. Since $\sqrt{2} \in L$ (this is easy to check) we consider the tower of fields:

$$K_{14} \subseteq K \subseteq L,$$

where $K = K_{14}(\sqrt{2})$. Then K/K_{14} and L/K are both quadratic extensions. The first one is visibly a quadratic extension and the second is $K(\sqrt{\mu})/K$ where $\mu = 2\sqrt{2} - 1 \in K$. Showing that L/K_{14} is an unramified extension is equivalent to showing that both K/K_{14} and L/K are unramified extensions (since ramification indices work in towers).

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_{K_{14}}$. We show that K/K_{14} is an unramified extension. Since $K = K_{14}(\sqrt{2})$ we can use case one of the above lemma to tell us that $\mathfrak{p}$ is unramified in K whenever $2 \notin \mathfrak{p}$ (since when $2 \notin \mathfrak{p}$ we have that $2u = 2.2 \notin \mathfrak{p}$ by definition of prime ideal). Now consider the case where $2 \in \mathfrak{p}$. We may rewrite K as $K_{14}(\sqrt{-7})$ since $\sqrt{-14} \in K_{14}$ and $\sqrt{2} \in K$. But now $-7 \notin \mathfrak{p}$ and writing $-7 = 1^2 - 4.2$ we see by part 2 of the previous lemma that $\mathfrak{p}$ is unramified. Thus K/K_{14} is an unramified extension.

We now only need to check that L/K is an unramified extension. We know that $L = K(\sqrt{\mu})$ where $\mu = 2\sqrt{2} - 1$. Letting $\mu' = -2\sqrt{2} - 1$ and noting that $\sqrt{\mu\mu'} = \sqrt{-7}$ we see that $\sqrt{\mu'} \in K$ (since $\sqrt{-7} \in K$ by the above). Thus $L = K(\sqrt{\mu}) = K(\sqrt{\mu'})$.

Again take a prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ and suppose $2 \notin \mathfrak{p}$. Then the fact that $\mu + \mu' = -2$ tells us that $\mu + \mu' \notin \mathfrak{p}$. But this implies that either one of μ, μ' does not lie in $\mathfrak{p}$ and in either case we can use claim 1 of the above lemma to show that $\mathfrak{p}$ is unramified in L.

If $2 \in \mathfrak{p}$ then $\mu = 2\sqrt{2} - 1 \notin \mathfrak{p}$ and after writing μ as $(1 + \sqrt{2})^2 - 4$, we may use claim 2 of the lemma to show that $\mathfrak{p}$ is unramified in L. This shows that L/K is unramified and we are done. □

We are now able to classify those p such that $p = x^2 + 14y^2$.

Corollary 5.2.3. *If $p \neq 2, 7$ is a rational prime then:*

$$p = x^2 + 14y^2 \iff \left(\frac{-14}{p}\right) = 1 \quad \text{and} \quad (a^2+1)^2 \equiv 8 \bmod p \quad \text{for some } a \in \mathbb{Z}.$$

Proof. We know that the Hilbert class field of $K_{14} = \mathbb{Q}(\sqrt{-14})$ is $L = K_{14}(\sqrt{2\sqrt{2} - 1})$ by the above. Thus the polynomial $f_{14}(x)$ in Corollary 5.1.5 can be taken to be the minimal polynomial of $\sqrt{2\sqrt{2} - 1}$ over $\mathbb{Q}$. This is easily checked to be $x^4 + 2x^2 - 7 = (x^2 + 1)^2 - 8$. The discriminant of this polynomial turns out to be $-2^{14}.7$ and so the only primes that are excluded by the theorem are 2 and 7. The result follows. □

To see a demonstration of this, first consider the prime $p = 23 = 3^2 + 14.1^2$. Checking the right hand side of the above result we can see that $\left(\frac{-14}{23}\right) = \left(\frac{9}{23}\right) = 1$ and that $a = 3$ is such that $(a^2 + 1)^2 \equiv 8 \bmod 23$.

To give an example of how the reverse implication works notice that the prime $p = 127$ is such that $\left(\frac{-14}{123}\right) = 1$. Also $a = 27$ is such that $(a^2 + 1)^2 \equiv 8 \bmod 127$. The result is verified in this case since we can write $127 = 1^2 + 14.3^2$.

The fact that we considered $n = 14$ in the above was irrelevant. Many Hilbert class fields of quadratic fields can be found by using the lemma and the general case splitting method above.

Since the invention of modern computer algebra systems it has been easier to compute Hilbert class fields with programs (using complex multiplication methods). The book [4] is an amazing book, detailing many computer algorithms for working out useful things in algebraic number theory.

Provided in Appendix C of this book are tables of Hilbert class field polynomials for all imaginary quadratic fields with discriminants between -3 and -451. We now know that these polynomials are useful in solving our problem (whenever n satisfies the conditions that we have been assuming).

One extra thing to note is the fact that there can be more than one such polynomial (a field extension is never generated by a unique element, different generators can also work). In the book the author provides a different polynomial to the one we found for the Hilbert class field of $\mathbb{Q}(\sqrt{-14})$ but this one works just as well as the one we found earlier.

We use this table now to give an example. We will find out exactly when $p = x^2 + 21y^2$. Take the number field $K_{21} = \mathbb{Q}(\sqrt{-21})$. It has discriminant -84 and ring of integers $\mathbb{Z}[\sqrt{-21}]$, again as expected. This means

that to solve the problem for $n = 21$, it is enough to find the defining polynomial for the Hilbert class field of K_{21}.

The table mentioned above tells us that for an imaginary quadratic field of discriminant -84, the corresponding polynomial is $x^4 - x^2 + 1$. This polynomial has discriminant 144 which is only divisible by the primes 2 and 3 and $n = 21$ is only divisible by the primes 3 and 7.

This immediately tells us that:

Corollary 5.2.4. *If $p \neq 2, 3, 7$ is a rational prime then:*

$$p = x^2 + 21y^2 \iff \left(\frac{-21}{p}\right) = 1 \quad \textit{and} \quad a^4 - a^2 + 1 \equiv 0 \bmod p \quad \textit{for some} \, a \in \mathbb{Z}.$$

To demonstrate this, let $p = 37$ and notice that $37 = 4^2 + 21.1^2$. On the other hand notice that $\left(\frac{-21}{37}\right) = \left(\frac{16}{37}\right) = 1$ and that $a = 8$ is such that $a^4 - a^2 + 1 \equiv 0 \bmod 37$.

Conversely choose the prime $p = 193$. Then by trial and error we find that $a = 49$ is a solution of $a^4 - a^2 + 1 \equiv 0 \bmod 193$ and also after calculation we find that that $\left(\frac{-84}{193}\right) = 1$. This suggests that 193 can be written in the form $x^2 + 21y^2$ and in fact it can since $193 = 2^2 + 21.3^2$.

Now that we have seen two examples we wonder what can be said about the case for general n. Here the ring $\mathbb{Z}[\sqrt{-n}]$ is not the ring of integers but is a structure known as an *order*. Technically an order of a quadratic number field K is a subring $\mathfrak{O}$ of K containing 1 that is also a free $\mathbb{Z}$-module of rank 2.

The ring of integers $\mathfrak{O}_K$ is itself an order and it can be shown that every order of K lies inside this one. Thus $\mathfrak{O}_K$ is called the *maximal order*. The index $f = [\mathfrak{O}_K : \mathfrak{O}]$ is called the *conductor* of the order $\mathfrak{O}$.

There is a notion of discriminant for orders. This is found in the same way and we get the connection $D = f^2 d_K$, where d_K is the discriminant of K.

Unfortunately not all orders are Dedekind domains so that prime ideal factorisation is not always unique. Most other properties of $\mathfrak{O}_K$ do transfer to all orders.

Unique factorisation of ideals can be restored if we consider a special set of ideals called *proper ideals*. These are ideals $\mathfrak{a}$ of $\mathfrak{O}$ that satisfy:

$$\{\alpha \in K \mid \alpha\mathfrak{a} \subseteq \mathfrak{a}\} = \mathfrak{O}.$$

It is known that we have unique factorisation of proper ideals coprime to $f\mathfrak{O}$ in terms of proper *prime* ideals coprime to $f\mathfrak{O}$.

We can construct a generalisation of the ideal class group, this time for an order:

$$C(\mathfrak{O}) = I(\mathfrak{O})/P(\mathfrak{O}).$$

Here $I(\mathfrak{O})$ is the group of proper fractional ideals of K with respect to the order $\mathfrak{O}$ (and similarly $P(\mathfrak{O})$ consists of the principal ones).

The order of this group is denoted $h(\mathfrak{O})$. This number (and specifically h_K) can be calculated in practice via a nice correspondence with binary quadratic forms. We will not go into this here.

We find that if we look at proper fractional ideals coprime to $f\mathfrak{O}$ we can form the groups $I(\mathfrak{O}, f)$ and $P(\mathfrak{O}, f)$ and we get the isomorphism:

$$I(\mathfrak{O}, f)/P(\mathfrak{O}, f) \cong I(\mathfrak{O})/P(\mathfrak{O}) = C(\mathfrak{O}).$$

The group on the left can be connected to fractional ideals of the maximal order $\mathfrak{O}_K$ by:

$$I(\mathfrak{O}, f)/P(\mathfrak{O}, f) \cong I_K(f\mathfrak{O}_K)/P_{K,\mathbb{Z}}(f\mathfrak{O}_K),$$

where $P_{K,\mathbb{Z}}(f\mathfrak{O}_K)$ are the principal ideals in $I_K(f\mathfrak{O}_K)$ generated by α such that $\alpha \equiv a \bmod f\mathfrak{O}_K$ for some $a \in \mathbb{Z}$ coprime to f.

The upshot here is that we have the inclusions:

$$P_{K,1}(f\mathfrak{O}_K) \subseteq P_{K,\mathbb{Z}}(f\mathfrak{O}_K) \subseteq I_K(f\mathfrak{O}_K),$$

telling us that $P_{K,\mathbb{Z}}(f\mathfrak{O}_K)$ is a congruence subgroup for the modulus $f\mathfrak{O}_K$ of K. By the existence theorem it now follows that there exists a field $K_{\mathfrak{O}}$ such that $K_{\mathfrak{O}}/K$ is Abelian and that:

$$C(\mathfrak{O}) \cong \mathrm{Gal}(K_{\mathfrak{O}}/K).$$

This field $K_{\mathfrak{O}}$ is called the *ring class field* of the order $\mathfrak{O}$. Note that when $\mathfrak{O} = \mathfrak{O}_K$ we get the Hilbert class field from earlier.

It can be proved with a little extra work that the solution to our problem for general n is basically the same as before. As usual we take $K_n = \mathbb{Q}(\sqrt{-n})$ and consider the order $\mathfrak{O} = \mathbb{Z}[\sqrt{-n}]$. We can show that the ring class field $K_{\mathfrak{O}}$ can be written as a finite extension of K_n of the form $K_n(\alpha)$, where α is some real algebraic integer. The polynomial $f_n(x)$ in our earlier solution can now be taken to be the minimal polynomial of this α over $\mathbb{Z}$. Of course there is something to prove here but these facts are omitted (the arguments here do not follow as easily as the earlier arguments).

As an illustration of the above discussion we consider the case $n = 27$ (this certainly does not fit the conditions we had to place on n earlier). Here it is a result that the ring class field corresponding to the order $\mathbb{Z}\left[\sqrt{-27}\right]$ of $K_{27} = \mathbb{Q}(\sqrt{-27})$ is $K_{27}(\sqrt[3]{2})$ (see p.184 of [3] for a proof of this).

So we get the following:

Corollary 5.2.5. *If $p \neq 2, 3$ is a rational prime then:*

$$p = x^2 + 27y^2 \iff p \equiv 1 \bmod 3 \quad \text{and} \quad a^3 \equiv 2 \bmod p \quad \text{for some } a \in \mathbb{Z}.$$

Proof. The ring class field here has a primitive element $\sqrt[3]{2}$ which has minimal polynomial $x^3 - 2$ over $\mathbb{Q}$. The discriminant of this polynomial turns out to be $-2^2.3^3$ and so the only primes that are excluded by the theorem are 2 and 3. Also by properties of the Legendre symbol and that fact that $p \neq 3$ we see that:

$$\left(\frac{-27}{p}\right) = 1 \iff \left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \bmod 3.$$

The result follows. □

As usual, we see examples of how this works both ways. Take the prime $p = 31$. This can be written in the form $x^2 + 27y^2$ by taking $x = 2$ and $y = 1$. Checking the right hand side we clearly see that $31 \equiv 1 \bmod 3$ and that $a = 11$ is such that $a^3 \equiv 2 \bmod 31$.

On the other hand take $p = 43 \equiv 1 \bmod 3$. Also $a = 9$ is such that $a^3 \equiv 2 \bmod 43$. We find that we can write $43 = 4^2 + 27.1^2$. This verifies the result above.

In chapter 6 of [4], the author lists algorithms that compute polynomials over $\mathbb{Z}$ whose roots can be used to generate the ring class field of a given quadratic field with respect to a given order. Again these are found by complex multiplication methods. Unfortunately, the author does not make tables of ring class fields (due to the obvious reason that there are many different possible orders, not just the ones of the form $\mathbb{Z}[\sqrt{-n}]$).

References

[1] S. Lang, *Algebraic Number Theory – 2nd edition,* Springer Graduate Texts in Mathematics, 1994.

[2] N. Childress, *Class Field Theory,* Springer Universitext, 2008.

[3] D. A. Cox, *Primes of the Form $x^2 + ny^2$,* Wiley, 1989.

[4] H. Cohen, *Advanced Topics in Computational Number Theory,* Springer Graduate Texts in Mathematics, 1993.

[5] G. F. B. Riemann, *On the Number of Primes Less Than a Given Magnitude,* `http://www.maths.tcd.ie/pub/HistMath/People/Riemann/Zeta/EZeta.pdf`, Translated by D. R. Wilkins, 1998.

[6] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein,* Springer Monographs in Mathematics, 2000.

[7] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem, 3rd edition,* A. .K. Peters, 2002