An overview of global class field theory

Daniel Fretwell

September 18, 2015

Contents

1 Introduction

Class field theory lies at the heart of modern number theory. It provides significant answers to significant questions and allows us to put certain difficult problems to rest. As a stepping stone to the more general Langlands program, it is important to appreciate this remarkable chapter in the theory of numbers.

In this overview we study the class field theory of number fields without main proofs. There are similar theories for local fields and function fields.

To explain the ideas of global class field theory we should first return to the roots of number theory. We have the following classical theorem of Fermat:

Theorem 1.1. *(Fermat) An odd prime p can be written as a sum of two squares if and only if $p \equiv 1 \bmod 4$.*

This theorem has many proofs. One can prove it using elementary techniques but the proof itself is not very satisfying and relies on quite a few non-obvious tricks. We can, however, prove this by using more general tools from algebraic number theory. Here the proof becomes something very intuitive and satisfying (in that it generalises to other situations).

We notice that the integer quadratic form $x^2 + y^2$ factorises as $(x + iy)(x - iy)$ over the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. It is this fact which links representation of prime numbers by this quadratic form with the factorisation properties of prime numbers in $\mathbb{Z}[i]$. So equivalent to the above theorem is the following:

Theorem 1.2. *An odd prime p factorises further in $\mathbb{Z}[i]$ if and only if $p \equiv 1 \bmod 4$.*

Fortunately we have general theorems in algebraic number theory that apply here, telling us when primes p factorise further in $\mathbb{Z}[i]$; namely this happens if and only if x^2+1 has a solution mod p. But this is the same as the Legendre symbol $\left(\frac{-1}{p}\right) = 1$, which gives the $p \equiv 1 \bmod 4$ condition we were looking for.

It is clear that other Diophantine problems may be solved in similar ways by exhibiting a ring similar to $\mathbb{Z}[i]$. However things are not so simple since factorisation is not always unique in such rings. For example if we wanted to solve the Diophantine equation $x^2+5y^2 = p$ for prime p we would have to invoke the ring $\mathbb{Z}[\sqrt{-5}]$, which certainly does not have unique factorisation $(6 = 2\times 3 = (1+\sqrt{-5})(1-\sqrt{-5}))$.

The significance of the Gaussian integers here is that they form the ring of integers of the number field $\mathbb{Q}(i)$. As the reader will probably know, the ring of integers of a number field K is a special subring $\mathfrak{O}_K$ that has unique factorisation on the level of ideals. Thus in $\mathfrak{O}_K$ every proper ideal $\mathfrak{a}$ has a unique factorisation into prime ideals:

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_g^{e_g}.$$

So we would like to have an accurate description of the prime ideal factorisation of $p\mathfrak{O}_K$, the ideal generated by p in $\mathfrak{O}_K$. Knowing this is equivalent to knowing how p factorises in the ring of integers (although this may now not be unique).

As mentioned above we have a general theorem that lets us study how $p\mathfrak{O}_K$ factorises in general rings of integers. It relates this to the factorisation of a certain polynomial $f(x) \bmod p$ (actually f is the minimal polynomial of a specific generator of the number field). But factorising polynomials mod p is non-trivial, even though it can be done in a finite amount of time.

The idea is to settle for a little less information. Rather than knowing the full factorisation of $p\mathfrak{O}_K$ we would like to just study the "factorisation type". This means knowing the number g of prime ideals in the factorisation, the ramification indices e_i and the inertia degrees $f_i := [\mathfrak{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$. There is a strict relationship between these numbers which will be mentioned soon. However in Galois extensions things will become quite a bit simpler so we shall work in those.

Let us return to the number field $\mathbb{Q}(i)$ and its ring of integers $\mathbb{Z}[i]$. We notice a few things:

- The only prime to ramify (i.e. have some $e_i > 1$) is the prime 2. This seems to be exactly the prime we omit when definitions and theorems concern only odd primes. In particular this is true with the definition of the Legendre symbol and the statement of quadratic reciprocity.
- The splitting behaviour of p is completely determined by $p \bmod 4$. This condition is only dependent on the arithmetic of $\mathbb{Z}$ not of the "larger" ring $\mathbb{Z}[i]$. This is quite special behaviour that can be observed in certain other settings.
- The modulus 4 itself is intriguing in that it is only divisible by the ramified prime. However we needed some non-trivial power to get an exact correspondence.

These three points are part of a more general behaviour. It is a part of class field theory to explain them. The Artin reciprocity law will show that this kind of behaviour holds in any *abelian* extension L/K of number fields. This simply means that we have a Galois extension with abelian galois group.

Why should we have to impose such a condition? It is not obvious why abelian extensions are at all important at first sight. The general idea is to try to associate to each prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ a conjugacy class of elements of $\mathrm{Gal}(L/K)$ that measure factorisation type of $\mathfrak{p}$ in $\mathfrak{O}_L$. However we will only be able to do this neatly for $\mathfrak{p}$ unramified in $\mathfrak{O}_L$. It now becomes obvious why the abelian condition is needed, since then we are really associating to each such $\mathfrak{p}$ a unique element of $\mathrm{Gal}(L/K)$. This will be called the *Frobenius element* of $\mathfrak{p}$ and will become very important in our studies.

The Artin reciprocity law will tell us things about the Frobenius elements; specifically how they are completely determined by the arithmetic of $\mathfrak{O}_K$ via mod $\mathfrak{m}$ behaviour. Implicitly this tells us that factorisation types are determined by mod $\mathfrak{m}$ behaviour too (where $\mathfrak{m}$ should be divisible only by ramified primes). Compare this to the above discussions when $L = \mathbb{Q}(i)$ and $K = \mathbb{Q}$.

It should be mentioned that, except for the largely unproven Langlands reciprocity law, the Artin reciprocity law is one of the most general ones that are proved to work. It can be used to prove all known reciprocity laws before it. We will see how we use it to prove the quadratic reciprocity law of Gauss.

We will also see the Existence theorem. This gives us the opposite side of the correspondence, that fixing mod $\mathfrak{m}$ behaviour for splitting somehow determines the field L. So really class field theory is telling us that abelian extensions of number fields are determined completely by the splitting behaviour you allow and vise versa.

Other avenues will be explored such as the Hilbert class field of a number field with applications to Diophantine problems such as representation of primes by quadratic forms such as $x^2 + ny^2$. We will see a generalisation of Dirichlet's theorem on primes in arithmetic progressions called the Ceboterev density theorem.

Finally the class field theory we introduce here is in terms of ideals. The modern views consider the theory in terms of ideles. The reader can read about this elsewhere once the ideal theory is built.

2 Recap of basic facts from algebraic number theory

To clarify the objects and tools we will need I should make a basic survey of classical algebraic number theory.

2.1 Number fields

Recall the definition of a number field.

Definition 2.1.1. A *number field* is a field K such that $[K : \mathbb{Q}]$ is finite.

Any such extension must be algebraic (this is easy to prove). Thus every $\alpha \in K$ must have a minimal polynomial defined over $\mathbb{Q}$. Clearing denominators we find α satisfies a polynomial over $\mathbb{Z}$. The monic ones are important.

Definition 2.1.2. The *ring of integers* of a number field is:

$$\mathfrak{O}_K = \{\alpha \in K \mid f(\alpha) = 0 \text{ for some monic } f(x) \in \mathbb{Z}[x]\}.$$

We may call elements of $\mathfrak{O}_K$ *integers*, reserving the term *rational integer* for elements of $\mathbb{Z}$.

As implied in the name this set will always be a subring of K although this is not straightforward to prove.

The ring of integers is a Dedekind domain. The importance of this is that the ring is Noetherian so that factorisation into irreducibles always exists (but is not necessarily unique). Also in a Dedekind domain maximal ideals and prime ideals are the same thing.

To reclaim unique factorisation we turn to ideals (since as mentioned in the introduction, we cannot guarantee unique factorisation of elements). It turns out that in any Dedekind domain the proper ideals have unique factorisation into prime ideals:

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_g^{e_g}$$

as mentioned in the introduction.

Now each $\mathfrak{p}_i$ is a prime ideal so is maximal (we are in a Dedekind domain). Thus the quotient $\mathfrak{O}_K/\mathfrak{p}_i$ is a field. In fact it is a finite field.

Why should this be so? Well each $\mathfrak{p}_i$ defines a prime ideal $\mathfrak{p}_i \cap \mathbb{Z}$ of $\mathbb{Z}$. But prime ideals of $\mathbb{Z}$ are of the form $p\mathbb{Z}$ for some rational prime p. Thus $\mathfrak{p}_i$ divides $p\mathfrak{O}_K$ for a unique prime p and so $\mathfrak{O}_K/\mathfrak{p}_i \subseteq \mathfrak{O}_K/p\mathfrak{O}_K$. But the latter contains finitely many elements (since $\mathfrak{O}_K$ turns out to be finitely generated as a $\mathbb{Z}$-module). Thus $\mathfrak{O}_K/\mathfrak{p}_i$ is finite. In fact we now know that it is a finite field of characteristic p, so must have p^{f_i} elements for some f_i.

Definition 2.1.3. The finite field $\mathfrak{O}_K/\mathfrak{p}_i$ is called the *residue field* of $\mathfrak{p}_i$, often denoted $\mathbb{F}_{\mathfrak{p}_i}$. The positive integer f_i is called the *intertia degree*. The positive integer e_i is called the *ramification degree* of $\mathfrak{p}_i$. We say that the ideal $\mathfrak{a}$ *ramifies* in $\mathfrak{O}_K$ (or in K) if some $e_i > 1$.

It is known that only finitely many primes ramify and one can find them by calculating the *different* or the *discriminant* of a number field. We shall not go into this here.

There is a quite a surprising relation between the numbers defined above:

Theorem 2.1.4. *Let K be a number field with ring of integers $\mathfrak{O}_K$. Then for any prime ideal factorisation:*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_g^{e_g}$$

we have that $\sum_{i=1}^{g} e_i f_i = [K : \mathbb{Q}]$.

This is quite a restrictive condition on the factorisation type of $\mathfrak{a}$. For example if $[K : \mathbb{Q}] = 2$ then it tells us that only three things can happen:

- $\mathfrak{a}$ is prime (i.e. $g = e = 1$, $f = 2$). Say $\mathfrak{a}$ is *inert*.
- $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2$ for two distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ (i.e. $e_1 = e_2 = f_1 = f_2 = 1$, $g = 2$). Say $\mathfrak{a}$ *splits*.
- $\mathfrak{a} = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$, so is ramified (i.e. $g = f = 1$, $e = 2$). Say $\mathfrak{a}$ *ramifies*.

Later we will see how the above theorem becomes even more restrictive when working in a Galois extension. Before we move onto general extensions of number fields we define a numerical norm of an ideal:

Definition 2.1.5. Given a proper ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ we define its *absolute norm* to be $N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|$.

Like the usual norms used in number theory this one is multiplicative and always gives a finite output. Notice that the norm of a prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ will be p^f, where f is the inertia degree and p is the unique prime in $\mathbb{Z}$ as defined above.

2.2 Relative extensions of number fields

We can now study what happens when we pass from one number field to a "larger" one. Suppose we take an extension L/K of number fields. Given any proper ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ we can extend it to an ideal $\mathfrak{a}\mathfrak{O}_L$ of $\mathfrak{O}_L$. In doing so we obtain a factorisation:

$$\mathfrak{a}\mathfrak{O}_L = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}...\mathfrak{q}_g^{e_g}.$$

Now each $\mathfrak{q}_i$ defines a prime ideal $\mathfrak{q}_i \cap \mathfrak{O}_K$ of $\mathfrak{O}_K$. It follows that the field $\mathbb{F}_{q_i} = \mathfrak{O}_L/\mathfrak{q}_i$ contains $\mathbb{F}_{\mathfrak{p}}$ as a subfield, where $\mathfrak{p}$ is the corresponding prime ideal of $\mathfrak{O}_K$. Thus the extension $\mathbb{F}_{\mathfrak{q}_i}/\mathbb{F}_{\mathfrak{p}}$ is a finite extension of finite fields. We know that this extension has degree p^{f_i} where p is the unique rational prime defined by $\mathfrak{q}_i \cap \mathbb{Z} = \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

In this fashion we may make some definitions similar to those in the previous subsection.

Definition 2.2.1. The positive integer f_i is also called the *intertia degree* of $\mathfrak{q}_i$ in K. When it is obvious which setting we are in we will just call it the inertia degree. The positive integer e_i is called the *ramification index* of $\mathfrak{a}$ in L. We say that $\mathfrak{a}$ *ramifies* in $\mathfrak{O}_L$ (or in L) if some $e_i > 1$.

The relationship between these numbers is similar to before:

Theorem 2.2.2. *As defined above the integers e_i, f_i and g satisfy $\sum_{i=1}^{g} e_i f_i = [L : K]$.*

We may also define a norm relative to the extension L/K as follows:

Definition 2.2.3. Given a proper prime ideal $\mathfrak{q}$ of $\mathfrak{O}_L$ we define its *relative norm* to be $N_{L/K}(\mathfrak{q}) = \mathfrak{p}^f$ where $\mathfrak{q} \cap \mathfrak{O}_K = \mathfrak{p}$. Extending multiplicatively we are able to define the relative norm of any proper ideal of $\mathfrak{O}_L$.

This norm will feature later in the statement of Artin reciprocity so it will be an important thing. Note that in studying the factorisation of $\mathfrak{a}\mathfrak{O}_L$ we are in some sense studying how certain elements of $\mathfrak{O}_K$ factorise further in $\mathfrak{O}_L$. This is what we saw in the introduction when we considered rational primes p and how their ideals factorise in "bigger" rings.

We have a major theorem that tells us how to factorise $\mathfrak{p}\mathfrak{O}_L$ for prime ideals $\mathfrak{p}$ of $\mathfrak{O}_K$. This theorem was alluded to in the introduction.

Theorem 2.2.4. *Let L/K be an extension of number fields with $L = K(\alpha)$ for some integer $\alpha \in \mathfrak{O}_L$ (such an α may always be found). Let $f(x)$ be the minimal polynomial of α over $\mathbb{Z}$. Suppose for a given prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ coprime to $[\mathfrak{O}_K : \mathbb{Z}[\alpha]]$ we have that:*

$$f(x) = \prod_{i=1}^{g} f_i(x)^{e_i} \bmod \mathfrak{p}$$

then:

$$\mathfrak{p}\mathfrak{O}_L = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}$$

where $\mathfrak{q}_i = \langle \mathfrak{p}, f_i(\alpha) \rangle$ are the prime ideals in the factorisation.

This is a very powerful result. It tells us that factorisation of ideals is similar to factorisation of polynomials. For quadratic extensions of the form $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ it tells us specifically that factorisation of (odd) p is really determined completely by the value of the Legendre symbol $\left(\frac{a}{p}\right)$. But quadratic reciprocity lets us turn these conditions into congruences for p mod $4a$. This is a small step towards the power of Artin reciprocity and it is roughly how the generalisation occurs. We will replace the role of the Legendre symbol by something more general that applies to other extensions of number fields. The Artin reciprocity law will then link this new creation to "congruence" conditions, just as the quadratic reciprocity law linked the Legnedre symbol with congruence conditions.

2.3 Fractional ideals and the ideal class group

How might one *measure* unique factorisation of elements in $\mathfrak{O}_K$? Well intuitively the point in introducing ideals was to consider *multiples* of elements as an object in its own right. The fact that certain prime ideal factors are non-principal is telling us that we are counting the multiples of an element that does not exist in the ring (but would contribute to unique factorisation in an extension ring). So really in Dedekind domains factorisation of elements is unique if and only if all ideals are principal (i.e. the domain is a PID).

Returning to our question it becomes clear that we may measure the (non)-uniqueness of factorisation of elements by discarding principal ideals from factorisations and looking for genuinely different prime ideals (ones that are not the same upto principal ideal multiples). This process can be achieved through creating a quotient group from ideals called the ideal class group. But to do this we need a group of ideals to mod out by.

It is immediate that for any number field K the set of ideals of $\mathfrak{O}_K$ *almost* forms a group under multiplication with identity being $\mathfrak{O}_K$ itself. We are simply missing inverses. The notion of fractional ideal allows us to do this. The way we proceed is to notice that ideals of $\mathfrak{O}_K$ are $\mathfrak{O}_K$-submodules of $\mathfrak{O}_K$. However instead we may use the entire number field K to take our submodules from. Hopefully in doing this we create objects that are invertible.

Definition 2.3.1. A *fractional ideal* of a number field K is an $\mathfrak{O}_K$ submodule of K.

We may write fractional ideals as $\alpha^{-1}\mathfrak{a}$ where $\alpha \in K^\times$. This is where the fractional nature arises. The fact that $\mathfrak{O}_K$ is a Dedekind domain helps to prove the following:

Theorem 2.3.2. *Every fractional ideal of K is invertible. Thus the set I_K of fractional ideals of K is an abelian group under multiplication. The principal fractional ideals form a subgroup denoted P_K.*

We can extend unique factorisation of ideals to fractional ideals. In doing so we are now guaranteed a prime ideal factorisation with possibly negative ramification indices.

As mentioned above we wish to measure the (non)-uniqueness of factorisation. We are now in a position to construct the ideal class group:

Definition 2.3.3. The *ideal class group* of a number field K is the abelian group I_K/P_K. Its order is the *class number* of K denoted h_K.

So we see that unique factorisation is equivalent to the class number being 1. Fortunately the class number of any number field is well defined. This is due to the remarkable fact that the ideal class group is a finite abelian group (not obvious). There are analytic formulae that allow us to find the class number of a given number field but we shall not go into these here.

The ideal class group will return later when we discover the Hilbert class field of a number field.

3 On the road to Artin reciprocity

Having made a survey of the basics we can now begin to delve into class field theory. For this we will need to consider only Galois extensions of number fields. This will not be too much of a problem since most of the nice Diophantine problems we try to solve are linked with Galois extensions.

Our progress will be as follows. First we will utilise the action of the Galois group on prime ideals. Secondly we will introduce special elements of the Galois group called Frobenius elements that describe the different factorisation types. Finally we will state the Artin reciprocity law via use of a special group homomorphism called the Artin map. This reciprocity law explains how the Frobenius elements are linked with a special notion of "congruence" for ideals.

Altogether this will give us quite an important connection between abelian extensions of a number field K and arithmetic of K (namely splitting types, "congruences" etc).

3.1 A special Galois action and Frobenius elements

Consider a Galois extension L/K of number fields. Given a prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ we have seen that we get a factorisation:

$$\mathfrak{p}\mathfrak{O}_L = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}...\mathfrak{q}_g^{e_g}.$$

As mentioned earlier we are not that fussed about finding the actual $\mathfrak{q}_i$'s but are content with knowing the e_i's, the f_i's and g. We could find the $\mathfrak{q}_i$'s given enough time.

One clever way to study a set is via a group action on that set. We are going to do exactly this.

Lemma 3.1.1. *The Galois group L/K acts on each of the sets $X_\mathfrak{p} = \{\mathfrak{q}_1, \mathfrak{q}_2, ..., \mathfrak{q}_g\}$ of prime ideal divisors of $\mathfrak{p}\mathfrak{O}_L$. Further the action is transitive.*

Proof. It is easy to see that for each $\sigma \in \mathrm{Gal}(L/K)$ the set $\sigma(\mathfrak{q}_i)$ is a prime ideal of $\mathfrak{O}_L$. Further notice that:

$$\mathfrak{p}\mathfrak{O}_L = \sigma(\mathfrak{p})\sigma(\mathfrak{O}_L) = \sigma(\mathfrak{p}\mathfrak{O}_L) = \sigma(\mathfrak{q}_1)^{e_1}\sigma(\mathfrak{q}_2)^{e_2}...\sigma(\mathfrak{q}_g)^{e_g}$$

so that by uniqueness of factorisation $\sigma(\mathfrak{q}_i) = \mathfrak{q}_j \in X$ for some j. Therefore this operation on X is well defined and the other group action axioms are easily checked.

It remains to check transitivity. This is omitted here but can be found in any good book on algebraic number theory (such as Lang).

□

This group action will tell us plenty about factorisation types. The following corollary already illuminates the situation.

Corollary 3.1.2. *If L/K is a Galois extension then for any factorisation of a prime ideal $\mathfrak{p} \subset \mathfrak{O}_K$ in $\mathfrak{O}_L$ we have that $e_1 = e_2 = ... = e_g$ (so we may call the common value e) and $f_1 = f_2 = ... = f_g$ (common value f). Thus $efg = [L : K]$.*

Proof. This is quite simple to prove. By transitivity of the group action it follows that for each i there exists $\sigma_i \in \mathrm{Gal}(L/K)$ such that $\sigma_i(\mathfrak{q}_i) = \mathfrak{q}_1$. But then uniqueness of factorisation tells us that $e_i = e_1$.

It is easy to see that the inertia degrees will be equal since σ_i is an automorphism. Also the fact that $\sum_{i=1}^{g} e_i f_i = [L:K]$ now reduces to $efg = [L:K]$. □

So in Galois extensions of number fields factorisations look nicer:

$$\mathfrak{p}\mathfrak{O}_L = (\mathfrak{q}_1\mathfrak{q}_2 ... \mathfrak{q}_g)^e$$

where $efg = [L:K]$.

Now that we have a group action we may study the sets $X_\mathfrak{p}$ by looking at stabilizer subgroups. Hopefully this will give an algebraic way to determine the splitting type of $\mathfrak{p}$ in L. Fix such a $\mathfrak{p}$ from now on.

Definition 3.1.3. Let L/K be a Galois extension of number fields. Given a fixed prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ and a prime ideal $\mathfrak{q}$ of $\mathfrak{O}_L$ such that $\mathfrak{q}|\mathfrak{p}\mathfrak{O}_L$ we define the *decomposition group* of $\mathfrak{q}$ to be:

$$D_\mathfrak{q} := \mathrm{stab}(\mathfrak{q}) = \{\sigma \in \mathrm{Gal}(L/K) \,|\, \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

We may now use the Orbit-Stabilizer theorem to provide a size for the Decomposition groups.

Lemma 3.1.4. *We have that* $|D_\mathfrak{q}| = ef$ *for all* $\mathfrak{q}|\mathfrak{p}\mathfrak{O}_L$.

Proof. This is easy since the action is transitive (so there is only one orbit containing g elements). The Orbit-Stabilizer theorem tells us that:

$$|D_\mathfrak{q}| = |\mathrm{stab}(\mathfrak{q})| = \frac{|G|}{|\mathrm{orb}(\mathfrak{q})|} = \frac{[L:K]}{g} = \frac{efg}{g} = ef.$$

Notice that we used the assumption that we were in a Galois extension. □

So this lemma tells us that tied up in these decomposition groups is all of the information we need on the factorisation type of the prime ideal $\mathfrak{p}$. If we know one of the decomposition groups then we can find g. We must work harder and find a way to extract the values of e and f.

The way we do this is to construct an epimorphism from $D_\mathfrak{q}$ into the Galois group of residue fields. The kernel will turn out to have size corresponding to the ramification index.

First notice that every $\sigma \in \mathrm{Gal}(L/K)$ induces an isomorphism:

$$\tilde{\sigma} : \mathbb{F}_\mathfrak{q} \longrightarrow \mathbb{F}_{\sigma(\mathfrak{q})}$$

$$x + \mathfrak{q} \longmapsto \sigma(x) + \sigma(\mathfrak{q}).$$

This is easy to prove and is left to the reader.

However we may now notice that specifically taking $\sigma \in D_\mathfrak{q}$ will induce an automorphism of $\mathbb{F}_\mathfrak{q}$. Further such automorphisms will fix elements of the subfield $\mathbb{F}_\mathfrak{p}$. So $\tilde{\sigma}$ will then be a well defined element of $\mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$.

The following theorem shows us how important this construction is:

Theorem 3.1.5. *The map:*

$$D_\mathfrak{q} \longrightarrow \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$$

$$\sigma \longmapsto \tilde{\sigma}$$

is an epimorphism of groups inducing an isomorphism:

$$D_\mathfrak{q}/I_\mathfrak{q} \cong \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}),$$

where $I_\mathfrak{q} = \{\sigma \in D_\mathfrak{q} \,|\, \sigma(x) \equiv x \bmod \mathfrak{q} \text{ for all } x \in \mathfrak{O}_L\}$.

Proof. Most of this can be checked easily. Proof of surjectivity is not very illuminating so will be omitted. Note that $I_\mathfrak{q}$ is just the kernel of the epimorphism. This gives the isomorphism. □

Definition 3.1.6. The group $I_{\mathfrak{q}}$ in the above is called the *inertia group* of $\mathfrak{q}$.

We will now see a simple corollary that shows how we can isolate the arithmetic data we want.

Corollary 3.1.7. *We have that $|I_{\mathfrak{q}}| = e$ and $|D_{\mathfrak{q}}/I_{\mathfrak{q}}| = f$ for each $\mathfrak{q}|\mathfrak{p}\mathfrak{O}_L$.*

Proof. This follows from the fact that the right hand side of the isomorphism above has order f by definition (since $\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}$ is a Galois extension of degree f). This proves the second claim and the first now follows since we already know that $|D_{\mathfrak{q}}| = ef$. □

So we have now managed to algebraically define subgroups of $\mathrm{Gal}(L/K)$ that measure arithmetic data regarding factorisation types. We can say more!

Recall that a finite extension of finite fields L/K has a cyclic Galois group, with canonical generator being the Frobenius automorphism $x \mapsto x^{|K|}$. The isomorphism above tells us that $D_{\mathfrak{q}}/I_{\mathfrak{q}}$ must also be cyclic and that there must be a unique element of this group corresponding to the Frobenius map in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$. This map is given by $x + \mathfrak{q} \mapsto x^{N(\mathfrak{p})} + \mathfrak{q}$ (since $N(\mathfrak{p}) = |\mathfrak{O}_K/\mathfrak{p}| = |\mathbb{F}_{\mathfrak{p}}|$ by definition).

Tying all of this together we get the following:

Theorem 3.1.8. *Let $\mathfrak{p}$ be a fixed prime ideal of $\mathfrak{O}_K$ and let $\mathfrak{q}$ be a fixed prime ideal of $\mathfrak{O}_L$ dividing $\mathfrak{p}\mathfrak{O}_L$. Then there exists an element $\sigma \in D_{\mathfrak{q}}$ that satisfies $\sigma(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{q}$ for all $x \in \mathfrak{O}_L$. The set of such elements forms a coset of $I_{\mathfrak{q}}$ in $D_{\mathfrak{q}}$.*

Further if $\mathfrak{p}$ is unramified in L then σ is a unique element of $D_{\mathfrak{q}}$.

Proof. Most of the work has been done. Notice that the congruential definition of σ matches the definition of the Frobenius given above (just it is now applied to elements of $\mathfrak{O}_L$ rather than cosets).

The second claim is a simple consequence of the isomorphism, since if $\mathfrak{p}$ is unramified in L then $|I_{\mathfrak{q}}| = e = 1$, so that:

$$D_{\mathfrak{q}} \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}).$$

□

Definition 3.1.9. In the above setup we call coset of such elements the *Frobenius coset* of $\mathfrak{q}$ in L/K. For unramified $\mathfrak{p}$ we may call the unique element the *Frobenius element* of $\mathfrak{q}$, denoted $\left(\frac{L/K}{\mathfrak{q}}\right)$.

We can immediately say something:

Lemma 3.1.10. *Let $\mathfrak{p}$ be unramified in L. The Frobenius element $\left(\frac{L/K}{\mathfrak{q}}\right)$ has order f in $D_{\mathfrak{q}}$ for all $\mathfrak{q}$ dividing $\mathfrak{p}\mathfrak{O}_L$.*

Further this Frobenius element is the identity automorphism if and only if $\mathfrak{p}$ "splits completely" in L (i.e. $e = f = 1$ and $g = [L : K]$).

Proof. The first claim is easy to see since by definition the Frobenius element of $\mathfrak{q}$ is a generator of $D_{\mathfrak{q}}$, this group being cyclic of order f (under the conditions on $\mathfrak{p}$).

The second claim follows from the fact that $\mathfrak{p}$ is unramified (so that $e = 1$) and that an element of a group has order 1 if and only if it is the identity. The fact that $g = [L : K]$ is then true since $efg = [L : K]$. □

This small lemma has told us a little about one particular factorisation type. We can now tell when $\mathfrak{p}$ splits completely, this being equivalent to all of the Frobenius elements of the $\mathfrak{q}$'s being the identity. It should be noted at this stage that we only know about the *order* of these elements in general, they are not necessarily equal as you run through the possible $\mathfrak{q}$'s.

The reason for such a bizarre looking notation is because Frobenius elements can be linked with Legendre symbols and other symbols defined for higher powers. Really the Legendre symbol $\left(\frac{a}{p}\right)$ is something akin to the Frobenius symbol for p relative to the extension $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$. Recall that when you first define the Legendre symbol you must do it for odd prime p not dividing a. These conditions are exactly what it means for p to ramify in $\mathbb{Q}(\sqrt{a})$ and it is no coincidence that these conditions are exactly what are required to get a well-defined Frobenius element!

We should study this further if we are going to want to study previous reciprocity laws in terms of Frobenius elements. Let us work out the Frobenius elements in $\mathbb{Q}(i)/\mathbb{Q}$. We will notice some huge similarities with some of the results mentioned in the introduction.

Example 3.1.11. In the extension $\mathbb{Q}(i)/\mathbb{Q}$ there is only one ramified prime. This is 2. So take an odd prime p and a prime ideal $\mathfrak{q}$ of $\mathbb{Z}[i]$ dividing $p\mathbb{Z}[i]$.

Recall that $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ is isomorphic to the cyclic group of order 2. This group is generated by complex conjugation which we will denote as τ.

Now for all $a, b \in \mathbb{Z}$ the Frobenius element of $\mathfrak{q}$ must satisfy:

$$\left(\frac{\mathbb{Q}(i)/\mathbb{Q}}{\mathfrak{q}}\right)(a+ib) \equiv (a+ib)^p \bmod \mathfrak{q},$$

since $N(p\mathbb{Z}) = |\mathbb{Z}/p\mathbb{Z}| = p$.

But $\mathbb{F}_{\mathfrak{q}}$ is a finite field of characteristic p so:

$$(a+ib)^p \equiv a^p + i^p b^p \equiv a + (-1)^{\frac{p-1}{2}} ib \bmod \mathfrak{q}.$$

Thus our Frobenius element is determined by the value of $(-1)^{\frac{p-1}{2}}$ (note that this is only dependent on p and not on $\mathfrak{q}$, this is something special which will be investigated soon).

So we see that:

$$\left(\frac{\mathbb{Q}(i)/\mathbb{Q}}{\mathfrak{q}}\right) = \begin{cases} \mathrm{id} & \text{if and only if } p \equiv 1 \bmod 4; \\ \tau & \text{if and only if } p \equiv 3 \bmod 4. \end{cases}$$

Notice the similarities with the splitting behaviour mentioned in the introduction (for odd prime p):

$$p \text{ splits in } \mathbb{Q}(i) \text{ if and only if } p \equiv 1 \bmod 4,$$

$$p \text{ is inert in } \mathbb{Q}(i) \text{ if and only if } p \equiv 3 \bmod 4.$$

However now we know (by the properties of the Frobenius element) that these factorisation types are *explained* by the values of the Frobenius element.

We could have proved these splitting behaviour facts by noting that the minimal polynomial of i over $\mathbb{Z}$ is x^2+1. Then Theorem 2.2.4 tells us that p factorises in $\mathbb{Q}(i)$ if and only if $\left(\frac{-1}{p}\right) = 1$, which is equivalent to $p \equiv 1 \bmod 4$ (by elementary number theory). But we no longer even have to do that, the Frobenius element has somehow got the values of the Legendre symbol encoded in it!

I promised you a connection with Legendre symbols and here it is. We found above that:

$$\left(\frac{\mathbb{Q}(i)/\mathbb{Q}}{\mathfrak{q}}\right)(a+ib) \equiv a + (-1)^{\frac{p-1}{2}} ib \bmod \mathfrak{q}.$$

The eagle eyed readers will notice that we can relate this to Legendre symbols using Euler's criterion, which tells us that:

$$(-1)^{\frac{p-1}{2}} \equiv \left(\frac{-1}{p}\right) \bmod p.$$

But the great thing here is that the Frobenius element is a purely algebraic thing, once worked out it will *determine* what $\left(\frac{-1}{p}\right)$ is. There is no dependence on knowing these values.

To make this specific we work in terms of representations. We may notice that the representation:

$$\rho : \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \longrightarrow \mathbb{C}^\times,$$

given by:

$$\rho(\mathrm{id}) = 1$$
$$\rho(\tau) = -1$$

satisfies:

$$\rho\left(\left(\frac{\mathbb{Q}(i)/\mathbb{Q}}{\mathfrak{q}}\right)\right) = \left(\frac{-1}{p}\right).$$

So viewed in the correct way the Frobenius elements for this extension really *are* the Legendre symbols. We have to move into the complex numbers in the correct way for the definitions to match up.

If done for a general quadratic extension $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ similar results hold (for odd prime p coprime to a) but with the Legendre symbol $\left(\frac{a}{p}\right)$. Again if we form the 1-dimensional representation of the Galois group that sends the non-trivial automorphism to -1 then we get a match between Frobenius elements and Legendre symbols similar to the above (for differing p).

Example 3.1.12. Choose an odd rational prime p. This time we will work with a cyclotomic extension $\mathbb{Q}(\zeta)/\mathbb{Q}$, where ζ is a primitive p-th root of unity. It is known that this is a degree $p-1$ Galois extension and that the only prime to ramify is p itself.

The elements of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ are as follows:

$$\sigma_i : \zeta \longmapsto \zeta^i,$$

for $i = 1, 2, ..., p-1$.

Take a rational prime $q \neq p$ and choose a prime ideal $\mathfrak{q}$ dividing $q\mathbb{Z}[\zeta]$. Again we know that the Frobenius element satisfies:

$$\left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{\mathfrak{q}}\right)(x) \equiv x^q \bmod \mathfrak{q}$$

for all $x \in \mathbb{Z}[\zeta]$.

Rather than working with an arbitary element of $\mathbb{Z}[\zeta]$ we should probably just look at the effect on ζ. A well known fact that can easily be proved is that the p-th roots of unity will be inequivalent mod $\mathfrak{q}$ (since $\mathfrak{q}$ does not divide $p\mathbb{Z}[\zeta]$).

But the left hand side of the above congruence for $x = \zeta$ must be ζ^j for some j (since we have an element of the Galois group acting on ζ).

We then have:

$$\zeta^j \equiv \zeta^q \bmod \mathfrak{q}$$

and the above fact forces $j \equiv q \bmod p$.

So we find that:

$$\left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{\mathfrak{q}}\right) = \sigma_q.$$

Again notice the independence of $\mathfrak{q}$ in these calculations.

As with quadratic extensions of $\mathbb{Q}$ we can now evoke arithmetic, since so far we have only worked algebraically. It would be nice to have results relating to modular arithmetic just as in the quadratic extension case.

We know (or can see) that:

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$$

via:

$$\sigma_a \longmapsto \bar{a}.$$

Thus the Frobenius elements are secretly determined by mod p behaviour. But we can say more. We know that the inertia degree f of q is equal to the order of the Frobenius element. Using the above isomorphism we see that f is also the order of q mod p (i.e. the smallest f such that $q^f \equiv 1 \bmod p$). This is something easily calculable and once found we know that $g = \frac{[\mathbb{Q}(\zeta):\mathbb{Q}]}{f} = \frac{p-1}{f}$ and so we could find g too.

In particular the primes that split completely are exactly the ones that satisfy $q \equiv 1 \bmod p$. These results can also be proved using basic algebraic number theory but here things fall out quite nicely.

As with the last example it is possible to link 1-dimensional representations of the Galois group with certain mod p Dirichlet characters. The correspondence is obvious here since we knew a priori that the Galois group had arithmetic significance (due to the isomorphism above). Since the groups are isomorphic

so must their character groups. There are also links with higher power symbols (generalisations of Legendre symbols to higher power residues).

In both this example and the previous one we have managed to explain splitting behaviour under one consistent theory using Frobenius elements. In each case we got simple congruence conditions which determined the splitting type. The hope is that in general similar results hold. However, it is not obvious how to evoke arithmetic. It just so happened in the quadratic and cyclotomic cases that arithmetic was readily available using our old knowledge of number theory and Galois theory. Also we have only studied nice extensions of $\mathbb{Q}$, but with another base field what should be the correct notion of "congruence"? The Artin reciprocity law will sort all of this out but the arithmetic will only be nice for extensions with *abelian* Galois group.

3.2 The Artin map for Abelian extensions

In the previous subsection we found that the Frobenius elements of the $\mathfrak{q}$'s were very good at telling us about the splitting type of a given prime ideal $\mathfrak{p}$ unramified in L. Surprisingly in both examples we found that there was absolutely no dependence on which $\mathfrak{q}$ we chose, all of the Frobenius elements were the same and depended only on $\mathfrak{p}$. This does not happen in general but can be explained.

First we have a relationship between the Frobenius elements of different $\mathfrak{q}$'s under the Galois action.

Theorem 3.2.1. *Let $\mathfrak{p}$ be unramified in L and let $\mathfrak{q}$ divide $\mathfrak{p}\mathfrak{O}_L$. Then for all $\sigma \in Gal(L/K)$ we have that:*

$$\left(\frac{L/K}{\sigma(\mathfrak{q})}\right) = \sigma\left(\frac{L/K}{\mathfrak{q}}\right)\sigma^{-1}.$$

Proof. This is a simple consequence of the definition of Frobenius element. □

So there is more structure to the Frobenius elements than first appears. For a fixed unramified $\mathfrak{p}$ they are not only elements of the same order but are conjugate. Actually we get a full conjugacy class in $\mathrm{Gal}(L/K)$.

It makes sense to associate to each $\mathfrak{p}$ a "Frobenius conjugacy class" of $\mathrm{Gal}(L/K)$. The Cebotarev density theorem (later) will tell us about the distribution of prime ideals $\mathfrak{p}$ according to their Frobenius conjugacy classes. This theorem is a far reaching generalisation of Dirichlet's theorem on primes in arithmetic progressions. In fact applying Cebotarev's theorem to cyclotomic extensions $\mathbb{Q}(\zeta)/\mathbb{Q}$ gives Dirichlet's theorem.

For now we note the following nice corollary:

Corollary 3.2.2. *If $Gal(L/K)$ is abelian then the Frobenius elements are all equal for a given unramified $\mathfrak{p}$.*

Proof. This is a simple consequence of the lemma and the fact that conjugacy classes in abelian groups consist of single elements. □

Definition 3.2.3. We call L/K an *abelian extension* if L/K is Galois and $\mathrm{Gal}(L/K)$ is abelian. In such a case we may denote the single Frobenius element attatched to all $\mathfrak{q}|\mathfrak{p}\mathfrak{O}_L$ by $\left(\frac{L/K}{\mathfrak{p}}\right)$.

It is exactly this reason why our previous examples were independent of the prime ideal $\mathfrak{q}$, we were in an abelian extension and so there was only a dependence on $\mathfrak{p}$. This has got us partway to our goal of describing splitting types of abelian extensions in terms of the arithmetic of K. We at least know that the Frobenius depends only on $\mathfrak{p}$ but have yet to find out exactly how. Maybe there are nice "congruence" conditions that determine the Frobenius element of $\mathfrak{p}$ in abelian extensions? We have seen evidence of this and will soon see general results confirming this.

Our first task in describing this will be to construct a group homomorphism. Given an abelian extension L/K we would like to study the map:

$$\{\text{unramified prime ideals } \mathfrak{p} \subseteq \mathfrak{O}_K\} \longrightarrow \mathrm{Gal}(L/K)$$

$$\mathfrak{p} \longmapsto \left(\frac{L/K}{\mathfrak{p}}\right).$$

However considering the set of prime ideals alone is not really the best idea since we have no group structure. We would like to introduce a group of ideals that we can safely find the Frobenius element of.

We could try using the group of fractional ideals I_K to define such a map but there is clearly a problem with this since this group contains ramified prime ideals. We must try and find a way to cut out the ramified primes. To do this we will invent the notion of modulus. The word modulus is used because such an object will provide the notion of congruence we need to describe the Frobenius elements.

For completeness sake I must mention that there is a notion of ramification for real embeddings of a number field too.

Given an extension of number fields L/K the embeddings $K \longrightarrow \mathbb{C}$ extend to make embeddings $L \longrightarrow \mathbb{C}$. Compare this with the extension of ideals from K into L. When extending you either get an embedding that has image in $\mathbb{R}$ or two complex conjugate embeddings with image not fully contained in $\mathbb{R}$. Amongst this behaviour the real embeddings $K \longrightarrow \mathbb{R}$ play a special role. In some extensions L/K real embeddings of K can extend to provide complex conjugate embeddings of L. We consider this occurrence a kind of ramification since in some sense, explained below, complex conjugate embeddings can be considered as equivalent.

The two notions of ramification can be explained as one if we move into valuation theory. Here different prime ideals offer different non-archimedean valuations on K (the $\mathfrak{p}$-adic valuations) and real/complex embeddings offer the usual archimedian valuations on K. It is for this reason that we consider real embeddings and conjugate pairs of complex embeddings as some kind of "infinite primes". The real infinite primes may ramify under the definition above. The old definition of ramification of primes fits into this framework when you view the prime ideals in the factorisation of $\mathfrak{p}\mathfrak{O}_L$ as giving extensions of non-archimedean valuations to L.

The point here is that real embeddings can be used to provide some kind of positivity condition on elements of a number field and we really need to consider these seriously. For example in most elementary theorems we favour positive prime numbers over their negative counterparts. This positivity is really determined by choosing to acknowledge the unique real embedding $\mathbb{Q} \longrightarrow \mathbb{R}$ but in other number fields there are different choices, for example in $\mathbb{Q}(\sqrt{2})$ there are two embeddings into $\mathbb{R}$:

$$\sigma_1 : a + b\sqrt{2} \longmapsto a + b\sqrt{2},$$
$$\sigma_2 : a + b\sqrt{2} \longmapsto a - b\sqrt{2}.$$

What should be the definition of positivity here? Should we allow only those elements that are positive in our number-line sense (i.e. such that $\sigma_1(\alpha) > 0$ only), should we allow only those elements such that $\sigma_2(\alpha) > 0$ or should we allow only those elements that satisfy both? The three cases create different positivity criteria. For example $1 + \sqrt{2}$ is positive in the first sense, negative in the second sense (since $1 - \sqrt{2} < 0$) and so is negative in the third sense.

There are some elements, such as $2 + \sqrt{2}$ that are positive under all real embeddings. Such elements are called *totally positive*. Similar behaviour occurs in other number fields.

We are now in the position to define what a modulus should be for a general number field.

Definition 3.2.4. A *modulus* of a number field K is a formal product $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ where $\mathfrak{m}_0$ is an ideal of $\mathfrak{O}_K$ and $\mathfrak{m}_\infty$ is a collection of real embeddings $K \longrightarrow \mathbb{R}$.

The key point of this is that each modulus creates a nice subgroup of the group of fractional ideals. Note that there is a notion of coprimality between fractional ideals of K, namely they are coprime if they share no prime ideal divisor in their prime ideal factorisations.

Theorem 3.2.5. *Given a modulus $\mathfrak{m}$ of K the set $I_K(\mathfrak{m}) = \{\mathfrak{a} \in I_K \mid \mathfrak{a}$ coprime to $\mathfrak{m}_0\}$ is a subgroup of I_K. It contains the set $P_{1,K}(\mathfrak{m}) = \{\langle\alpha\rangle \in P_K \mid \alpha \equiv 1 \bmod \mathfrak{m}_0$ and $\sigma(\alpha) > 0$ for all $\sigma \in \mathfrak{m}_\infty\}$ as a subgroup.*

Now consider an arbitrary abelian extension L/K. It has a finite set of ramified primes (maybe infinite ones too). If we package them all together to form a modulus $\mathfrak{m}$ then the group $I_K(\mathfrak{m})$ should be something we are able to define the Frobenius element on. We can simply do this by extending multiplicatively from the definition on prime ideals, using the unique factorisation of fractional ideals into prime ideals.

It is now apparent that we have a map:

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

Definition 3.2.6. Given an abelian extension of number fields L/K and a modulus $\mathfrak{m}$ of K divisible by all ramified primes of K in L the map $\Phi_{\mathfrak{m}}$ is called the *Artin map* of L/K with respect to $\mathfrak{m}$.

This map is of importance in class field theory in that it contains all of the info on splitting types. On the right we have information about Frobenius elements whereas on the left we have fractional ideals of K. It is clear at once that this map is a homomorphism (although proving this again uses the abelian nature of the Galois group). If we could use it to form an isomorphism then we would be able to completely describe Frobenius elements in terms of classes of ideals of K, hence describing splitting types in terms of such classes. This would give a very beautiful connection that explains all previous findings.

We already know that Frobenius elements in abelian extensions somehow depend on the arithmetic of the base field but such an isomorphism would tell us *exactly* how this dependence goes. The Artin reciprocity law will explain this now.

3.3 Artin Reciprocity

We expect the group $P_{1,K}(\mathfrak{m})$ defined above to lie in the kernel of a suitable Artin map. Compare this with the situation for cyclotomic extensions $\mathbb{Q}(\zeta)/\mathbb{Q}$ done earlier (where ζ is a primitive nth root of unity). Here we found that p splits completely in such fields if and only if $p \equiv 1 \bmod n$. This is the same as saying that the kernel of the Artin map for the modulus $\mathfrak{m} = \langle n \rangle \infty$ contains $P_{1,\mathbb{Q}}(\mathfrak{m})$ (in fact it equals this).

The Artin reciprocity law tells us more than this. As discussed earlier it will tell us the exact kernel, which will describe exactly how the Frobenius elements depend on congruence conditions:

Theorem 3.3.1. *(Artin Reciprocity Law) Let L/K be an abelian extension of number fields. Suppose $\mathfrak{m}$ is a modulus of K divisible only by primes that ramify in L. Then:*

1. *The Artin map $\Phi_{\mathfrak{m}}$ is a surjective homomorphism.*
2. *If the powers of the prime ideals in $\mathfrak{m}$ are big enough then we are able to guarantee that $ker(\Phi_{\mathfrak{m}})$ is a **congruence subgroup** for $\mathfrak{m}$, meaning that:*

$$P_{1,K}(\mathfrak{m}) \subseteq ker(\Phi_{\mathfrak{m}}) \subseteq I_K(\mathfrak{m})$$

   *so that $I_K(\mathfrak{m})/ker(\Phi_{\mathfrak{m}})$ is a **generalised ideal class group** for $\mathfrak{m}$ (the definition of this is a quotient $I_K(\mathfrak{m})/H$ where H contains $P_{1,K}(\mathfrak{m})$).*
3. *Further, for such an $\mathfrak{m}$ we have that $ker(\Phi_{\mathfrak{m}}) = P_{1,K}(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$, giving an isomorphism:*

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

This theorem is one of the cornerstones of 20th century number theory. It describes how the arithmetic of abelian extensions L/K of number fields really depends entirely on the arithmetic of K, via "mod $\mathfrak{m}$" relationships. In the next section we will see a rough converse of this theorem that allows us to set in stone a correspondence between abelian extensions of K and generalised ideal class groups.

4 The existence theorem

As usual let K be a number field. The existence theorem asks the following question, "Given a modulus $\mathfrak{m}$, can we find a number field L such that L/K is an abelian extension satisfying the behaviour contained in the Artin reciprocity law?". Fortunately the answer is yes.

Theorem 4.0.2. *(Existence theorem) Let K be a number field and $\mathfrak{m}$ be any modulus of K. Then for each congruence subgroup H of $\mathfrak{m}$, there exists a number field L such that L/K is abelian, $\mathfrak{m}$ is divisible by the ramified primes of this extension and:*

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

This theorem and the Artin reciprocity law together sets in stone a rough correspondence between finite abelian extensions of K and generalised ideal class groups, with the choice of modulus roughly playing the role of choice of ramification.

As we saw earlier the splitting behaviour of unramified primes of $\mathbb{Q}(i)/\mathbb{Q}$ is completely determined by $p \bmod 4$. This can be produced in many different ways via classical results on sums of squares or via simple Frobenius calculations (which is really the Artin reciprocity law in action). The existence theorem helps to tell us another non-trivial fact; that any finite abelian extension of $\mathbb{Q}$ with ramified prime 2 and with splitting properties completely determined by $p \bmod 4$ **must** be $\mathbb{Q}(i)/\mathbb{Q}$.

The correspondence we have seen in this example is not quite exact in general, the field produced by the existence theorem is not always unique. Different modulus choices can give the same field (increasing the powers of the primes in the modulus does not change the overall ramification of the field we get). This is cleared up in the more modern approach when using ideles.

4.1 Ray class fields and the Hilbert class field

The existence theorem tells us lots of great things since we are free to choose the modulus and the congruence subgroup and produce a field L with prescribed properties.

In particular for a fixed modulus $\mathfrak{m}$ we may choose the congruence subgroup $H = P_{1,K}(\mathfrak{m})$. Then the existence theorem guarantees the existence of a number field $K_\mathfrak{m}$ such that $K_\mathfrak{m}/K$ is an abelian extension whose ramified primes are the only ones to divide $\mathfrak{m}$ and is such that $I_K(\mathfrak{m})/P_{1,K}(\mathfrak{m}) \cong \mathrm{Gal}(K_\mathfrak{m}/K)$. Further this field must be unique (although this is not obvious).

Definition 4.1.1. The field $K_\mathfrak{m}$ is called the *ray class field* of K with respect to $\mathfrak{m}$.

It is clear that any other congruence subgroup H for $\mathfrak{m}$ produces a field lying strictly inside $K_\mathfrak{m}$ (since the corresponding $I_K(\mathfrak{m})/H$ is isomorphic to a subgroup of $I_K(\mathfrak{m})/P_{1,K}(\mathfrak{m})$ and so by the Artin isomorphism is isomorphic to a subgroup of $\mathrm{Gal}(K_\mathfrak{m}/K)$, which by Galois theory corresponds to a subfield of $K_\mathfrak{m}$).

Thus the ray class fields $K_\mathfrak{m}$ are really maximal abelian extensions of K, unramified with respect to the primes not appearing in $\mathfrak{m}$.

In particular let $\mathfrak{m} = \langle 1 \rangle$, the trivial modulus. Then we are guaranteed the existence of a field $K_{\langle 1 \rangle}$ such that $K_{\langle 1 \rangle}/K$ is the maximal unramified abelian extension of K.

Definition 4.1.2. The *Hilbert class field* of a number field K is the field $K_{\langle 1 \rangle}$ defined above.

The Artin isomorphism tells us that for the Hilbert class field:

$$I_K/P_K \cong \mathrm{Gal}(K_{\langle 1 \rangle}/K).$$

Notice the appearance of the classical ideal class group here. We find the following nice properties:

Lemma 4.1.3. *The Hilbert class field is a degree h_K extension of K (recall h_K is the class number of K). Also a prime ideal $\mathfrak{p} \in \mathfrak{O}_K$ splits completely in the Hilbert class field if and only if $\mathfrak{p}$ is principal.*

Proof. Using the isomorphism above it is clear that $|\mathrm{Gal}(K_{\langle 1 \rangle}/K)| = h_K$ and since we are working with Galois extensions, $[K_{\langle 1 \rangle} : K] = |\mathrm{Gal}(K_{\langle 1 \rangle}/K)|$.

For the second claim recall that the primes that split completely are exactly the ones in the kernel of the Artin map. However here the kernel is P_K. This gives the result. □

Corollary 4.1.4. *The following are equivalent:*

1. $K = K_{\langle 1 \rangle}$.
2. $h_K = 1$.
3. $\mathfrak{O}_K$ *is a PID (or equivalently a UFD).*

Proof. If $K = K_{\langle 1 \rangle}$ then by the lemma $h_K = 1$. The converse of this also holds since the only degree 1 extension of K is K. Thus $K = K_{\langle 1 \rangle}$ is equivalent to $h_K = 1$.

But we have already seen that $\mathfrak{O}_K$ being a PID is equivalent to $h_K = 1$. The result follows. □

Example 4.1.5. The field $\mathbb{Q}$ has class number 1 (since $\mathbb{Z}$ is a PID). Thus the Hilbert class field of $\mathbb{Q}$ is itself. This shows the well known fact that every extension $K/\mathbb{Q}$ with $K \neq \mathbb{Q}$ has non-trivial ramification.

The same can be said for $\mathbb{Q}(i)$ (since $\mathbb{Z}[i]$ is a PID). This tells us the less obvious fact that every proper extension of $\mathbb{Q}(i)$ has non-trivial ramification too.

The natural question to ask is how to construct ray class fields and more specifically Hilbert class fields without having to resort to ad hoc methods. Unfortunately not much is known.

An answer to this question has been provided when $K = \mathbb{Q}$ or an imaginary quadratic field. The first case of this is easy to describe. Essentially the answer is that cyclotomic number fields are in some sense maximal amongst all abelian extensions of $\mathbb{Q}$. We will work on proving this now.

Note that the only possible moduli of $\mathbb{Q}$ are of the form $\langle m \rangle$ or $\langle m \rangle \infty$ for positive integer m (there is only one embedding of $\mathbb{Q}$ into $\mathbb{C}$, the identity one and this is real). We only have to consider positive m since in $\mathbb{Z}$ the element $-m$ is associate to m and so generates the same ideal as m.

Ramification at ∞ is simple to describe here, it simply means that the extension field L of $\mathbb{Q}$ is not contained inside $\mathbb{R}$ (in other words the identity embedding extends to complex conjugate embeddings on L).

Theorem 4.1.6. *Let ζ be a primitive mth root of unity for a positive integer m. We have that:*

$$\mathbb{Q}_{\langle m \rangle \infty} = \mathbb{Q}(\zeta)$$

and

$$\mathbb{Q}_{\langle m \rangle} = \mathbb{Q}(\zeta + \zeta^{-1}) \subset \mathbb{R}.$$

Proof. It is easy to see that:

$$I_{\mathbb{Q}}(\langle m \rangle \infty)/P_{1,\mathbb{Q}}(\langle m \rangle \infty) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$$

and

$$I_{\mathbb{Q}}(\langle m \rangle)/P_{1,\mathbb{Q}}(\langle m \rangle) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}/\{\pm 1\}.$$

Thus the field $\mathbb{Q}_{\langle m \rangle \infty}$ is a degree $\phi(m)$ extension of $\mathbb{Q}$ which is unramified at all primes not dividing m. We know that $\mathbb{Q}(\zeta)$ satisfies these properties and so by uniqueness must be the right field. The same argument shows the second equality. □

The following famous theorem now follows:

Corollary 4.1.7. *(Kronecker-Weber theorem) Let L be a number field such that $L/\mathbb{Q}$ is an abelian extension. Then $L \subseteq \mathbb{Q}(\zeta)$ for some primitive root of unity ζ.*

Proof. Consider the modulus $\mathfrak{m}$ consisting of the ramified primes of $L/\mathbb{Q}$. Then $L \subseteq \mathbb{Q}_{\mathfrak{m}}$ by maximality of $\mathbb{Q}_{\mathfrak{m}}$. But by the above theorem we see that no matter what $\mathbb{Q}_{\mathfrak{m}}$ actually is it must lie inside $\mathbb{Q}(\zeta)$ for some primitive root of unity ζ. □

For imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ the situation is a bit more complicated. It was found also by Kronecker that the ray class fields in this case are constructed by first producing an elliptic curve with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-d})$, then adjoining the j-invariant of such a curve along with values of Weber functions at $\mathfrak{m}$-torsion points on the curve (where $\mathfrak{m}$ is the modulus in question). In particular the Hilbert class field is constructed by just adjoining the j-invariant. It is not too difficult to produce an elliptic curve with such complex multiplication so this construction is not difficult in practice.

After studying these two cases, Kronecker observed that the ray class fields are constructed by adjoining special values of analytic functions. In the case $K = \mathbb{Q}$ we adjoined values of $f(z) = e^{2\pi i z}$ at rational numbers to get nth roots of unity and in the case $K = \mathbb{Q}(\sqrt{-d})$ we adjoined special values of the j-function and the Weber functions. Kronecker believed that a similar process should be considered in order to construct ray class fields of a general number field. This "conjecture" falls under the description of Kronecker's Jugendtraum (his *dream of youth*). So far very little has been proved in this direction, only the two cases mentioned above have been solved in general.

5 Applications of global class field theory

5.1 The Cebotarev density theorem

In this section we will see a theorem that in some sense widely generalises the following well known theorem:

Theorem 5.1.1. *(Dirichlet's theorem on primes in arithmetic progressions) Let a, n be positive integers with $n > 1$ and a coprime to n. Then there are infinitely many primes congruent to $a \bmod n$.*

It is quite simple to prove special cases of this theorem for small n. In most elementary number theory courses you see proofs for $n = 2$ (i.e. Euclid's original theorem on infinitude of primes) and usually some of the cases $n = 3, 4, 6, 8$. However the general theorem resists such attacks as studied in these courses. Dirichlet was the first to prove this theorem by using analytical tools. For a fixed n he invented Dirichlet L-series from characters of the finite abelian group $(\mathbb{Z}/n\mathbb{Z})^\times$ lifted to $\mathbb{Z}$. Then by making a nice linear combination of these series he was able to essentially show that $\sum_{p \equiv a \bmod n} \frac{1}{p}$ diverges, which implies the theorem.

We can rephrase this theorem in terms of Frobenius elements.

Theorem 5.1.2. *(Dirichlet rephrased) Let ζ be a primitive nth root of unity for some integer $n > 1$. Then for each integer a coprime to n there are infinitely many primes p satisfying $\left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{p\mathbb{Z}}\right) = \sigma_a$.*

In other words if you pick any element of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ then it is a Frobenius element for infinitely many primes in $\mathbb{Z}$. We can see how this is equivalent to the original version of the theorem since by earlier calculations $\left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{p\mathbb{Z}}\right) = \sigma_p$ and $\sigma_p = \sigma_a$ is equivalent to $p \equiv a \bmod n$.

The Cebotarev density theorem generalises this restatement of Dirichlet's theorem to all Galois extensions of number fields (not necessarily abelian ones).

Theorem 5.1.3. *(Cebotarev density theorem) Let L/K be a Galois extension of number fields. Then each conjugacy class in $Gal(L/K)$ appears as the Frobenius class for infinitely many prime ideals $\mathfrak{p}$ of $\mathfrak{O}_K$.*

In particular for abelian extensions each element of $Gal(L/K)$ appears as the Frobenius element for infinitely many prime ideals $\mathfrak{p}$ of $\mathfrak{O}_K$.

This is really a weak form of the full Cebotarev density theorem. The full form goes on to describe the distribution of such prime ideals according to their Frobenius classes. There is a well defined notion of "density" for such sets of prime ideals and it turns out that the prime ideals with a Frobenius class of size k in $\mathrm{Gal}(L/K)$ should account for $\frac{k}{[L:K]}$ of all prime ideals (of course this is not really a quantative statement since there are infinitely many prime ideals, it should be taken asymptotically).

For abelian extensions we always have $k = 1$ so really Cebotarev is saying that, for such extensions, if we discard the finitely many ramified primes then the rest of the primes are distributed uniformly between elements of $\mathrm{Gal}(L/K)$ with probability $\frac{1}{[L:K]}$. In other words each element of $\mathrm{Gal}(L/K)$ occurs as a Frobenius element and a particular one occurs as often as any other.

In particular for cyclotomic extensions $\mathbb{Q}(\zeta)/\mathbb{Q}$ we see that not only are there infinitely many primes congruent to $a \bmod n$ (for a coprime to n) but that all primes not dividing n are uniformly distributed between the classes of $(\mathbb{Z}/n\mathbb{Z})^\times$. The chances of a given prime p being congruent to $a \bmod n$ for a fixed a coprime to n is $\frac{1}{[\mathbb{Q}(\zeta):\mathbb{Q}]} = \frac{1}{\phi(n)}$. There is no dependence on a.

For example a randomly chosen odd prime is as likely to be congruent to 1 mod 4 as it is of being congruent to 3 mod 4, there is no favoured congruence class mod 4 for primes to belong to.

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

As mentioned in the introduction it has been known since the time of Fermat that an odd prime can be written as a sum of two squares if and only if $p \equiv 1 \bmod 4$. Perhaps less well known is his study of primes which can be written in the form $x^2 + 2y^2$ or $x^2 + 3y^2$. He found congruence conditions for these too.

Naturally we would like to generalise and study the representation of primes by $x^2 + ny^2$ for any positive integer n. The reasons for only considering positive n will become clear soon. Suffice to say we wish to land ourselves in an imaginary quadratic field.

Historically there were many discoveries that led to partial solutions of this problem. The crowning glory was the theory of binary quadratic forms, studied mainly by Gauss and Lagrange. Their ideas were not to study this one quadratic form but all positive definite quadratic forms with integer coefficients and the same discriminant. The representation of numbers by one particular form is then heavily related to the whole set of numbers represented by all such forms. There are nice group theoretical arguments hiding in the background here which is outlined in Cox's excellent book *Primes of the form $x^2 + ny^2$*.

However the theory mentioned above is not enough to solve this problem generally, we must turn to class field theory to get a full solution. To show why we first turn the problem into an algebraic one.

Lemma 5.2.1. *Let p be unramified in $\mathbb{Q}(\sqrt{-n})$. Then $p = x^2 + ny^2$ if and only if p splits into distinct, conjugate, principal prime ideals in $\mathbb{Z}[\sqrt{-n}]$.*

Proof. This is easy to see in both directions by using the factorisation $x^2 + ny^2 = (x + y\sqrt{-n})(x - y\sqrt{-n})$ in $\mathbb{Z}[\sqrt{-n}]$. □

Now we have to be careful here since $\mathbb{Z}[\sqrt{-n}]$ is not always the ring of integers of $\mathbb{Q}(\sqrt{-n})$, so we cannot immediately determine congruence conditions for which p split in this fashion (we might not even have unique factorisation of ideals!).

We will deal with the n such that we do get the ring of integers, namely squarefree $n \equiv 1 \bmod 4$. For such n we know that if p is odd and coprime to n then p splits in $\mathbb{Z}[\sqrt{-n}]$ if and only if the Legendre symbol $\left(\frac{-n}{p}\right) = 1$. However in the above lemma there is more information since we must have splitting into **principal** ideals that are conjugate. We know that all p with $\left(\frac{-n}{p}\right) = 1$ will split but not necessarily into principal ideals. However when the ring of integers $\mathbb{Z}[\sqrt{-n}]$ is a PID this condition is automatically true. So we get the following:

Theorem 5.2.2. *If $n \equiv 1 \bmod 4$ is squarefree and $\mathbb{Z}[\sqrt{-n}]$ is a PID then for odd p coprime to n we have $p = x^2 + ny^2$ if and only if $\left(\frac{-n}{p}\right) = 1$.*

In particular we get the old results of Fermat:

Corollary 5.2.3. *If p is an odd prime then $p = x^2 + y^2$ if and only if $p \equiv 1 \bmod 4$. Also $p = x^2 + 2y^2$ if and only if $p \equiv 1, 3 \bmod 8$.*

If $p \neq 3$ then $p = x^2 + 3y^2$ if and only if $p \equiv 1 \bmod 3$.

This corollary only highlights the simplest uses of the theorem, but there are other PID's out there that also apply. However we are still interested in getting a general solution. It is clear that we need to dispose of certain congruence classes of primes such that $\left(\frac{-n}{p}\right) = 1$ in order to get a complete solution for non-PID's. In order to do this we must also find out which p split into principal conjugate ideals.

The idea is to invoke the Hilbert class field to get a full answer since we know principal ideals are exactly the ones to split completely in this field!

Theorem 5.2.4. *Suppose p and n are as above. Then $p = x^2 + ny^2$ if and only if p splits completely in $\mathbb{Q}(\sqrt{-n})_{\langle 1 \rangle}$.*

See Cox for the proof. It is along the lines of the remark made above but slightly non-trivial. You can also create and test your own examples by looking up tables of Hilbert class fields.

We know how to study splitting behaviour using classical means, if we have the minimal polynomial $f(x)$ of a generator for the extension $\mathbb{Q}(\sqrt{-n})_{\langle 1 \rangle}/\mathbb{Q}$ then we simply require that $f(x) \equiv 0 \bmod p$ has an integer solution in order for $p\mathfrak{O}_{\mathbb{Q}(\sqrt{-n})}$ to split completely in the extension $\mathbb{Q}(\sqrt{-n})_{\langle 1 \rangle}/\mathbb{Q}(\sqrt{-n})$ plus the Legendre condition $\left(\frac{-n}{p}\right) = 1$ in order for p to split in the extension $\mathbb{Q}(\sqrt{-n})/\mathbb{Q}$.

Tying this together we get the following:

Corollary 5.2.5. *Let n be as above and α be a real integral generator for $\mathbb{Q}(\sqrt{-n})_{\langle 1\rangle}/\mathbb{Q}$. Take $f(x)$ to be the minimal polynomial of α over $\mathbb{Q}$ (actually because α is integral it will belong to $\mathbb{Z}[x]$).*

Then for any odd prime p not dividing n or the discriminant of f we have that $p = x^2 + ny^2$ if and only if $\left(\frac{-n}{p}\right) = 1$ and $f(x) \equiv 0 \bmod p$ has an integer solution.

We need the extra condition for p not dividing the discriminant of f in order to avoid the polynomial being separable mod p. This is an extra ramification condition coming from the extension to the Hilbert class field.

For values of n other than the ones we have considered the problem can still be solved and the reader is referred to Cox's book once again. Unfortunately for such n the ring $\mathbb{Z}[\sqrt{-n}]$ is no longer the ring of integers so may not have unique factorisation, even on the level of ideals. However these rings have enough structure to exploit what we want and are known as *orders*. Cox constructs the so called *Ring class fields*, generalisations of the ray class fields we saw earlier but attatched to orders (in fact $\mathfrak{O}_K$ is itself an order, the maximal one, and ring class fields here are the same as ray class fields).

5.3 Quadratic reciprocity

Gauss' law of Quadratic reciprocity is one of the most profound results in elementary number theory. It is reputed to be a theorem that has a high number of known proofs. Classically it is proved using lattice point methods but this method does not generalise well. In this section we see a proof using Frobenius elements.

Both proofs rely on the fact that the cyclotomic field $\mathbb{Q}(\zeta_p)$ has a unique quadratic subfield $K^{(p)}$ for any odd prime p. We can prove this fact easily:

Theorem 5.3.1. *The field $K^{(p)}$ exists and is unique for any odd prime p.*

Proof. The extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois. We saw earlier that it's Galois group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$ via:

$$\sigma_a \longmapsto \bar{a}.$$

However the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, which is even (since p is odd). Thus is has a unique subgroup of index 2, the subgroup of quadratic residues mod p (the even powers of the generator of this cyclic group). Let $H^{(p)}$ be the image of this group in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Thus by Galois theory there must exist a unique subfield $K^{(p)} \subset \mathbb{Q}(\zeta_p)$ of degree 2 that is the fixed field of $H^{(p)}$. □

In fact Gauss was able to find this field explicitly by creating a primitive version of what are today known as Gauss sums.

Theorem 5.3.2. *The field $K^{(p)} = \mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{\frac{p-1}{2}} p$.*

Proof. It is clear that this is a quadratic extension of $\mathbb{Q}$ so it remains to prove the inclusion $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$. In order to do so we construct an element of the cyclotomic field whose square is p^*.

Let:

$$S = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a \in \mathbb{Q}(\zeta_p).$$

This is an example of a Gauss sum, as mentioned above. A tedious calculation, which can be found in Lang, shows that:

$$S^2 = p^*,$$

hence $S = \pm\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$, proving the inclusion (in fact Gauss was able to determine the sign of S). □

Gauss sums have, since creation, become useful in many areas of maths. We can attach them to any Dirichlet character. In fact there is a proof of quadratic reciprocity using only the properties of the particular Gauss sum we constructed above.

We are now in a position to see the quadratic reciprocity law proved using Frobenius elements. We will only prove the version for odd prime values in the Legendre symbol but the supplementary laws for $\left(\frac{2}{p}\right)$ and $\left(\frac{-1}{p}\right)$ can also be proved by similar methods.

Theorem 5.3.3. *(Gauss' law of quadratic reciprocity) Let p, q be distinct odd primes. Then:*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof. We prove the equivalent theorem that $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$. Suppose that $\left(\frac{q}{p}\right) = 1$, then q is a quadratic residue mod p and so $\sigma_q \in H^{(p)}$. Hence σ_q fixes the field $K^{(p)}$.

However $\sigma_q = \left(\frac{\mathbb{Q}(\zeta_p)/\mathbb{Q}}{q\mathbb{Z}}\right)$ is the Frobenius element of q (since q is distinct from p it is unramified, hence it has a unique Frobenius element).

Thus (since restriction to an abelian subsextension preserves Frobenius elements):

$$\mathrm{id}_{K^{(p)}} = \sigma_q|_{K^{(p)}} = \left(\frac{\mathbb{Q}(\zeta_p)/\mathbb{Q}}{q\mathbb{Z}}\right)\Bigg|_{K^{(p)}} = \left(\frac{K^{(p)}/\mathbb{Q}}{q\mathbb{Z}}\right).$$

So now we know that q splits completely in $K^{(p)}$ since q is unramified here and has trivial Frobenius element for the extension $K^{(p)}/\mathbb{Q}$. Even better we know that $K^{(p)} = \mathbb{Q}(\sqrt{p^*})$ and by classical results we know that for q to split in this quadratic field we must have that $\left(\frac{p^*}{q}\right) = 1$.

It is easy to rewrite the above to prove that if $\left(\frac{q}{p}\right) = -1$ then $\left(\frac{p^*}{q}\right) = -1$ and so we are done. □

The above proof is an ingenious use of Galois theory and properties of Frobenius elements. However it doesn't really capture the full story of what is really going on here. We just happened to be lucky enough that we knew enough about the fields we were dealing with. If one tries to generalize to higher reciprocity laws then this proof will not be so easy to recapture. For starters, what fields should replace $K^{(p)}$ and $\mathbb{Q}(\zeta_p)$? In the next section we show how the Artin reciprocity law provides a more general view of the landscape of higher reciprocity laws.

5.4 Higher reciprocity laws

What we really showed in the above proof is that the two homomorphisms $\left(\frac{\cdot}{p}\right)$ and $\left(\frac{p^*}{\cdot}\right)$ behave in the same way. In fact in showing this we actually discover that as Kronecker symbols these homomorphisms are connected too (on appropriate groups). We will see exactly how the Artin reciprocity law makes this explicit and provides similar notions for higher power symbols.

Our first task is to produce a generalization of the Legendre symbol to higher power settings. A naive approach would be to consider defining for a coprime to n the symbol $\left(\frac{a}{p}\right)_n$ to be 1 if a is an n-th power mod p and -1 otherwise (just like the Legendre symbol).

It turns out that such a symbol, although arithmetically interesting, cannot be studied too easily. The reason is essentially the fact that we are not using enough roots of unity to distinguish the ways of "not being an n-th power".

To see why we need more nth roots of unity let us first consider the elementary theory of the Legendre symbol. If a is not divisible by odd prime p then Fermat's little theorem tells us that $a^{p-1} \equiv 1 \bmod p$. It is this congruence that implies $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$ and the cyclic nature of $(\mathbb{Z}/p\mathbb{Z})^\times$ gives Euler's criterion, that $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$. The real point here is that the definition of the Legendre symbol could really be taken to be defined by this congruence rather than forced by other definitions. If we approach things this way round then we define the Legendre symbol to be the unique square root of unity given by $a^{\frac{p-1}{2}} \bmod p$. Unfortunately for higher n-th powers this doesn't work because $p-1$ is not necessarily divisible by n and so such a congruence wouldn't even make sense in $\mathbb{Z}$ most of the time.

However after extending our number field $\mathbb{Q}$ in the hopes to make such a symbol definable we realise that we must create a field containing the n-th roots of unity and we must no longer work in the residue fields $\mathbb{F}_p$ but in the extended residue fields $\mathbb{F}_\mathfrak{p}$.

Mixing this together we see that we may define an n-th power residue symbol as follows.

1. Let K be a number field containing the n-th roots of unity and select a prime ideal $\mathfrak{p}$ coprime to $\langle n \rangle$ (this is the "odd prime" condition on the original Legendre symbol denominator).

2. Given any $\alpha \in \mathfrak{O}_K$ such that $\alpha \not\equiv 0 \bmod \mathfrak{p}$ we see that the analogue of Fermat's little theorem holds in $\mathbb{F}_\mathfrak{p}$, i.e. that $\alpha^{N(\mathfrak{p})-1} \equiv 1 \bmod \mathfrak{p}$. The condition on α corresponds to a not divisible by p in the original Legendre symbol definition (where in that case $\mathfrak{O}_K = \mathbb{Z}$).

3. It turns out that $n | N(\mathfrak{p}) - 1$ always, something not true when working in $\mathbb{Z}$. So we know that $\alpha^{\frac{N(p)-1}{n}} \equiv \zeta_n^i \bmod \mathfrak{p}$ for some $i \in \{0, 1, \ldots, n-1\}$ (where ζ_n is a primitive n-th root of unity).

4. However the n-th roots of unity can be shown to be distinct mod $\mathfrak{p}$ and so there is a *unique* n-th root of unity satisfying the above congruence.

5. Define the n-th power residue symbol to be $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = \zeta_n^i$ so that by definition it is the unique n-th root of unity satisfying $\alpha^{\frac{N(\mathfrak{p})-1}{n}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \bmod \mathfrak{p}$.

It turns out that like the Legendre symbol this new symbol measures n-th power behaviour mod $\mathfrak{p}$. If $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = 1$ then there is $\beta \in \mathfrak{O}_K$ such that $\alpha \equiv \beta^n \bmod \mathfrak{p}$ and if it is any other root of unity then there is no β. Essentially what we are saying now is that there is more than one way to fail to be an n-th power, dependent on which residue class $\alpha^{\frac{N(\mathfrak{p})-1}{n}} \bmod \mathfrak{p}$ lands in.

The residue symbols have properties extending from those of the Legendre symbol. For example each $\left(\frac{\cdot}{\mathfrak{p}}\right)_n$ satisfies $\left(\frac{\alpha\beta}{\mathfrak{p}}\right)_n = \left(\frac{\alpha}{\mathfrak{p}}\right)_n \left(\frac{\beta}{\mathfrak{p}}\right)_n$ wherever defined. Also we have the familiar congruence property, if $\alpha \equiv \beta \bmod \mathfrak{p}$ then $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = \left(\frac{\beta}{\mathfrak{p}}\right)_n$.

One major thing to note is that we can extend these residue symbols multiplicatively to form symbols where the denominator is any ideal coprime to $\langle n \rangle$. This is akin to the transformation from Legendre symbol to Kronecker symbol. In making this extension we now see that for a fixed $\alpha \in \mathfrak{O}_K$ the map $\left(\frac{\alpha}{\cdot}\right)_n$ is a homomorphism of the group $I_K(\mathfrak{m})$ into μ_n, the group of n-th roots of unity (where $\mathfrak{m}$ is any modulus of K with ideal part $\mathfrak{m}_0 = \langle n\alpha \rangle$). The question is, what are the kernel and image of this map? If we knew these then we would know lots of information of arithmetical significance, for example it would tell us which prime ideals α is an n-th power residue in.

After reading all of the above thoroughly it should remind you of the process we went through to obtain the artin maps $I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K)$. We first defined Frobenius symbols for unramified primes and then extended multiplicatively. Is it possible that we have really just done essentially the same thing twice in disguise. The answer is yes, but not in generality. In defining an Artin map we need an abelian extension L/K. We have the field K but what should L be taken to be in order to make ends meet?

It turns out that the correct field to take to replicate the $\left(\frac{\alpha}{\cdot}\right)_n$ map is the field $L = K(\sqrt[n]{\alpha})$. The great thing about extensions of the form $K(\sqrt[n]{\gamma})/K$ is that they are abelian (in fact cyclic) and their Galois groups inject into μ_n.

Why is this? Well if $\sigma \in \mathrm{Gal}(K(\sqrt[n]{\gamma})/K)$ then $\sigma(\sqrt[n]{\gamma}) = \zeta_n^i \sqrt[n]{\gamma}$ for some $i \in \{0, 1, \ldots, n-1\}$. So the map:

$$\phi : \mathrm{Gal}(K(\sqrt[n]{\gamma})/K) \longrightarrow \mu_n$$

given by:

$$\sigma \longmapsto \frac{\sigma(\sqrt[n]{\gamma})}{\sqrt[n]{\gamma}} = \zeta_n^i$$

is an injective homomorphism.

This fills in the last piece of the puzzle, we can now compare images of the Artin map for $K(\sqrt[n]{\alpha})/K$ and the residue symbols $\left(\frac{\alpha}{\cdot}\right)_n$ by using this injection into μ_n. This is the subject of the weak reciprocity law:

Theorem 5.4.1. *(Weak Reciprocity Law) Let K be a number field containing the n-th roots of unity. Choose $\alpha \in \mathfrak{O}_K$ and let $\mathfrak{m}$ be a modulus containing the primes dividing $\langle n\alpha \rangle$. Assume also that $\mathfrak{m}$ is big enough to*

guarantee that ker($\Phi_{\mathfrak{m}}$) is a congruence subgroup for $\mathfrak{m}$. Then we have (relative to the extension $K(\sqrt[n]{\alpha})/K$) that:

$$\phi(\Phi_{\mathfrak{m}}) = \left(\frac{\alpha}{\cdot}\right)_n.$$

In other words for each $\mathfrak{a} \in I_K(\mathfrak{m})$:

$$\left(\frac{K(\sqrt[n]{\alpha})/K}{\mathfrak{a}}\right)(\sqrt[n]{\alpha}) = \left(\frac{\alpha}{\mathfrak{a}}\right)_n \sqrt[n]{\alpha}.$$

Let $G = im(\phi) \subset \mu_n$. Then the residue symbol map induces a surjective homomorphism:

$$\left(\frac{\alpha}{\cdot}\right)_n : I_K(\mathfrak{m})/P_{1,K}(\mathfrak{m}) \longmapsto G.$$

Proof. The first claim is easy to prove. It suffices to prove it only for prime ideals $\mathfrak{p}$ in place of $\mathfrak{a}$ (by multiplicativity). Take a prime $\mathfrak{q}$ lying above $\mathfrak{p}$ in our extension. In this case:

$$\left(\frac{K(\sqrt[n]{\alpha})/K}{\mathfrak{a}}\right)(\sqrt[n]{\alpha}) \equiv \sqrt[n]{\alpha}^{N(\mathfrak{p})} = \sqrt[n]{\alpha}^{(N(\mathfrak{p})-1)}\sqrt[n]{\alpha} = \alpha^{\frac{N(\mathfrak{p})-1}{n}}\sqrt[n]{\alpha} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \sqrt[n]{\alpha} \bmod \mathfrak{q}.$$

Both sides of this congruence are numbers of the form $\zeta_n^i \sqrt[n]{\alpha}$. However the n-th roots of unity are distinct mod $\mathfrak{q}$ and so equality must occur.

The second part of the theorem needs the Artin reciprocity law. Since the modulus $\mathfrak{m}$ was chosen to satisfy the correct conditions we see that the Artin map gives an isomorphism:

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m})/\ker(\Phi_{\mathfrak{m}}) \longrightarrow \mathrm{Gal}(K(\sqrt[n]{\alpha})/K).$$

Composing with ϕ and gives us an isomorphism:

$$\phi(\Phi_{\mathfrak{m}}) : I_K(\mathfrak{m})/\ker(\Phi(\mathfrak{m})) \cong G$$

which by the above is also induced by the residue symbol $\left(\frac{\alpha}{\cdot}\right)$.

Now since $\ker(\mathfrak{m})$ is a congruence subgroup for $\mathfrak{m}$ we know that $P_{1,K}(\mathfrak{m}) \subseteq \ker(\mathfrak{m})$. This means that $\left(\frac{\alpha}{\cdot}\right)$ induces a surjective homomorphism $I_K(\mathfrak{m})/P_{1,K}(\mathfrak{m}) \longrightarrow G$ as required.

□

Note the similarities with the examples in section 3. Back then we proved a special case of the first part of the above theorem. Also notice that we actually proved something a lot stronger than the second part, we induced an isomorphism but this involved the kernel of the Artin map which is not something that is easy to work with in practice (even though it is known). We settle for a surjective homomorphism instead.

Let us show how the quadratic reciprocity law follows from weak reciprocity:

Proof. Once again we turn to the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$. Choose the modulus $\mathfrak{m} = \langle p \rangle \infty$. We have already seen that with respect to the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, $\mathfrak{m}$ is a suitable modulus to make $\ker(\Phi_{\mathfrak{m}})$ into a congruence subgroup. This implies that the same $\mathfrak{m}$ will do the same job for the subextension $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$.

The other conditions of the weak reciprocity theorem are satisfied and so $\left(\frac{p^*}{\cdot}\right)$ induces a surjective homomorphism:

$$\left(\frac{p^*}{\cdot}\right) : I_{\mathbb{Q}}(\mathfrak{m})/P_{1,\mathbb{Q}}(\mathfrak{m}) \longmapsto \mu_2 = \{\pm 1\}.$$

However we also saw earlier that $I_{\mathbb{Q}}(\mathfrak{m})/P_{1,\mathbb{Q}}(\mathfrak{m}) \equiv (\mathbb{Z}/p\mathbb{Z})^\times$ so we induce a surjective homomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mu_2$. However only one such homomorphism exists since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. We know it in another disguise as the Legendre symbol map $\left(\frac{\cdot}{p}\right)$. Hence the two maps must agree for any given input and quadratic reciprocity is proved. □

There is a strong reciprocity law that tells you exactly how to work out the relationship between the residue symbols but this requires more local considerations (Hilbert symbols). See Cox for details. I will simply state some of the higher reciprocity laws that arise once the strong reciprocity law is known.

Theorem 5.4.2. *(Cubic reciprocity) Working in $K = \mathbb{Q}(\zeta_3)$ (which has $\mathfrak{O}_K = \mathbb{Z}[\zeta_3]$, a PID) we have for all primes in $\mathfrak{O}_K$ satifsying $\alpha, \beta \equiv 2 \bmod \langle 3 \rangle$ (i.e. primary primes):*

$$\left(\frac{\alpha}{\langle\beta\rangle}\right)_3 = \left(\frac{\beta}{\langle\alpha\rangle}\right)_3.$$

As with quadratic reciprocity there are supplementary laws for units and ramified primes in the residue symbol.

The fact that α, β have to be primary is no restriction, every ideal in $\mathfrak{O}_K$ is principal and those coprime to $\langle 3 \rangle$ have a unique primary generator (i.e. every generator is associate to one that is $2 \bmod \langle 3 \rangle$). Then the multiplicativity of the residue symbols means any residue symbol can be calculated by using the reciprocity laws and the supplementary laws.

Theorem 5.4.3. *(Quartic reciprocity) Working in $K = \mathbb{Q}(i)$ (which has $\mathfrak{O}_K = \mathbb{Z}[i]$, a PID) we have for all primes in $\mathfrak{O}_K$ satisfying $\alpha, \beta \equiv 1 \bmod -2 + 2i = (1+i)^3$ (i.e. primary primes):*

$$\left(\frac{\alpha}{\langle\beta\rangle}\right)_4 = \left(\frac{\beta}{\langle\alpha\rangle}\right)_4 (-1)^{\frac{N(\alpha)-1}{4}\frac{N(\beta)-1}{4}}.$$

There are supplementary laws for this one too which can be found in Cox. We can also recover Eisenstein reciprocity by working with $K = \mathbb{Q}(\zeta_p)$ for odd prime p but this is left to the reader.