# XV

# Algebraic NT II: Galois and Ramification Theory

# Part XV: Contents

# 59 Things Galois

## §59.1 Motivation

*Prototypical example for this section:* $\mathbb{Q}(\sqrt{2})$ *and* $\mathbb{Q}(\sqrt[3]{2})$.

The key idea in Galois theory is that of *embeddings*, which give us another way to get at the idea of the "conjugate" we described earlier.

Let $K$ be a number field. An **embedding** $\sigma\colon K \hookrightarrow \mathbb{C}$, is an *injective field homomorphism*: it needs to preserve addition and multiplication, and in particular it should fix 1.

> **Question 59.1.1.** Show that in this context, $\sigma(q) = q$ for any rational number $q$.

**Example 59.1.2** (Examples of embeddings)

(a) If $K = \mathbb{Q}(i)$, the two embeddings of $K$ into $\mathbb{C}$ are $z \mapsto z$ (the identity) and $z \mapsto \overline{z}$ (complex conjugation).

(b) If $K = \mathbb{Q}(\sqrt{2})$, the two embeddings of $K$ into $\mathbb{C}$ are $a + b\sqrt{2} \mapsto a + b\sqrt{2}$ (the identity) and $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ (conjugation).

(c) If $K = \mathbb{Q}(\sqrt[3]{2})$, there are three embeddings:

- The identity embedding, which sends $1 \mapsto 1$ and $\sqrt[3]{2} \mapsto \sqrt[3]{2}$.
- An embedding which sends $1 \mapsto 1$ and $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$, where $\omega$ is a cube root of unity. Note that this is enough to determine the rest of the embedding.
- An embedding which sends $1 \mapsto 1$ and $\sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}$.

I want to make several observations about these embeddings, which will form the core ideas of Galois theory. Pay attention here!

- First, you'll notice some duality between roots: in the first example, $i$ gets sent to $\pm i$, $\sqrt{2}$ gets sent to $\pm\sqrt{2}$, and $\sqrt[3]{2}$ gets sent to the other roots of $x^3 - 2$. This is no coincidence, and one can show this occurs in general. Specifically, suppose $\alpha$ has minimal polynomial
$$0 = c_n\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0$$
where the $c_i$ are rational. Then applying any embedding $\sigma$ to both sides gives
$$\begin{aligned} 0 &= \sigma(c_n\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0) \\ &= \sigma(c_n)\sigma(\alpha)^n + \sigma(c_{n-1})\sigma(\alpha)^{n-1} + \cdots + \sigma(c_1)\sigma(\alpha) + \sigma(c_0) \\ &= c_n\sigma(\alpha)^n + c_{n-1}\sigma(\alpha)^{n-1} + \cdots + c_1\sigma(\alpha) + c_0 \end{aligned}$$
where in the last step we have used the fact that $c_i \in \mathbb{Q}$, so they are fixed by $\sigma$. *So, roots of minimal polynomials go to other roots of that polynomial.*

- Next, I want to draw out a contrast between the second and third examples. Specifically, in example (b) where we consider embeddings $K = \mathbb{Q}(\sqrt{2})$ to $\mathbb{C}$. The image of these embeddings lands entirely in $K$: that is, we could just as well have looked at $K \to K$ rather than looking at $K \to \mathbb{C}$. However, this is not true in (c): indeed $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, but the non-identity embeddings have complex outputs!

  The key difference is to again think about conjugates. Key observation:

  > **The field $K = \mathbb{Q}(\sqrt[3]{2})$ is "deficient" because the minimal polynomial $x^3 - 2$ has two other roots $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$ not contained in $K$.**

  On the other hand $K = \mathbb{Q}(\sqrt{2})$ is just fine because both roots of $x^2 - 2$ are contained inside $K$. Finally, one can actually fix the deficiency in $K = \mathbb{Q}(\sqrt[3]{2})$ by completing it to a field $\mathbb{Q}(\sqrt[3]{2}, \omega)$. Fields like $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{2})$ which are "self-contained" are called *Galois extensions*, as we'll explain shortly.

- Finally, you'll notice that in the examples above, *the number of embeddings from $K$ to $\mathbb{C}$ happens to be the degree of $K$*. This is an important theorem, Theorem 59.3.1.

In this chapter we'll develop these ideas in full generality, for any field other than $\mathbb{Q}$.

## §59.2 Field extensions, algebraic extension, and splitting fields

*Prototypical example for this section:* *$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is an extension, $\mathbb{C}$ is an algebraic extension of any number field.*

First, we define a notion of one field sitting inside another, in order to generalize the notion of a number field.

**Definition 59.2.1.** Let $K$ and $F$ be fields. If $F \subseteq K$, we write $K/F$ and say $K$ is a **field extension** of $F$.

Thus $K$ is automatically an $F$-vector space (just like $\mathbb{Q}(\sqrt{2})$ is automatically a $\mathbb{Q}$-vector space). The **degree** is the dimension of this space, denoted $[K : F]$. If $[K : F]$ is finite, we say $K/F$ is a **finite (field) extension**.

That's really all. There's nothing tricky at all.

> **Question 59.2.2.** What do you call a finite extension of $\mathbb{Q}$?

Degrees of finite extensions are multiplicative.

**Theorem 59.2.3** (Field extensions have multiplicative degree)
Let $F \subseteq K \subseteq L$ be fields with $L/K$, $K/F$ finite. Then

$$[L : K][K : F] = [L : F].$$

*Proof.* Basis bash: you can find a basis of $L$ over $K$, and then expand that into a basis $L$ over $F$. (Diligent readers can fill in details.) □

Next, given a field (like $\mathbb{Q}(\sqrt[3]{2})$) we want something to embed it into (in our case $\mathbb{C}$). So we just want a field that contains all the roots of all the polynomials. Let's agree that a field $E$ is **algebraically closed** if every polynomial with coefficients in $E$ is a product of linear polynomials in $E$, with the classic example is:

**Example 59.2.4** ($\mathbb{C}$)
$\mathbb{C}$ is algebraically closed.

A major theorem is that any field $F$ can be extended to an algebraically closed one $\overline{F}$; since all roots of polynomials in $\overline{F}[x]$ live in $\overline{F}$, in particular so do all roots of polynomials in $F[x]$. Here is the result:

**Theorem 59.2.5** (Algebraic closures)
Any field $F$ has algebraically closed field extensions. In fact, there is a unique such extension which is minimal by inclusion, called the **algebraic closure** and denoted $\overline{F}$. (Here "minimal" means any other algebraically closed extension of $F$ contains an isomorphic copy of $\overline{F}$.) It has the property that every element of $\overline{F}$ is indeed the root of some polynomial with coefficients in $F$.

**Example 59.2.6** ($\overline{\mathbb{R}} = \overline{\mathbb{C}} = \mathbb{C} \supsetneq \overline{\mathbb{Q}}$)
$\mathbb{C}$ is the algebraic closure of $\mathbb{R}$ (and itself). But the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ (i.e. the set of algebraic numbers) is a proper subfield of $\mathbb{C}$ (some complex numbers aren't the root of any rational-coefficient polynomial).

Usually we won't care much about what these extensions look like, and merely be satisfied they exist. Often we won't even use the algebraic closure, just any big enough field; for example, when working with a polynomial $f$ with $\mathbb{Q}$-coefficients, we simply consider roots of $f$ as elements of $\mathbb{C}$ for convenience and concreteness, even though it may be less wasteful to use the smaller $\overline{\mathbb{Q}}$ in place of $\mathbb{C}$.

## §59.3 Embeddings into algebraic closures for number fields

Now that I've defined all these ingredients, I can prove:

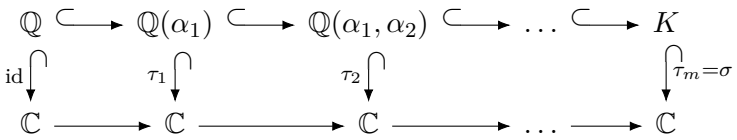
**Theorem 59.3.1** (The $n$ embeddings of a number field)
Let $K$ be a number field of degree $n$. Then there are exactly $n$ field homomorphisms $K \hookrightarrow \mathbb{C}$, say $\sigma_1, \dots, \sigma_n$ which fix $\mathbb{Q}$.

**Remark 59.3.2** — Note that a nontrivial homomorphism of fields is necessarily injective (the kernel is an ideal). This justifies the use of "$\hookrightarrow$", and we call each $\sigma_i$ an **embedding** of $K$ into $\mathbb{C}$.

*Proof.* This is actually kind of fun! Recall that any irreducible polynomial over $\mathbb{Q}$ has distinct roots (Lemma 54.1.2). We'll adjoin elements $\alpha_1, \alpha_2, \dots, \alpha_m$ one at a time to $\mathbb{Q}$, until we eventually get all of $K$, that is,

$$K = \mathbb{Q}(\alpha_1, \dots, \alpha_n).$$

Diagrammatically, this is




First, we claim there are exactly

$$[\mathbb{Q}(\alpha_1) : \mathbb{Q}]$$

ways to pick $\tau_1$. Observe that $\tau_1$ is determined by where it sends $\alpha_1$ (since it has to fix $\mathbb{Q}$). Letting $p_1$ be the minimal polynomial of $\alpha_1$, we see that there are $\deg p_1$ choices for $\tau_1$, one for each (distinct) root of $p_1$. That proves the claim.

Similarly, given a choice of $\tau_1$, there are

$$[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)]$$

ways to pick $\tau_2$. (It's a little different: $\tau_1$ need not be the identity. But it's still true that $\tau_2$ is determined by where it sends $\alpha_2$, and as before there are $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)]$ possible ways.)

Multiplying these all together gives the desired $[K : \mathbb{Q}]$. □

**Remark 59.3.3 —** The primitive element theorem actually implies that $m = 1$ is sufficient; we don't need to build a whole tower. This simplifies the proof somewhat.

It's common to see expressions like "let $K$ be a number field of degree $n$, and $\sigma_1, \dots, \sigma_n$ its $n$ embeddings" without further explanation. The relation between these embeddings and the Galois conjugates is given as follows.

**Theorem 59.3.4** (Embeddings are evenly distributed over conjugates)
Let $K$ be a number field of degree $n$ with $n$ embeddings $\sigma_1, \dots, \sigma_n$, and let $\alpha \in K$ have $m$ Galois conjugates over $\mathbb{Q}$.

Then $\sigma_j(\alpha)$ is "evenly distributed" over each of these $m$ conjugates: for any Galois conjugate $\beta$, exactly $\frac{n}{m}$ of the embeddings send $\alpha$ to $\beta$.

*Proof.* In the previous proof, adjoin $\alpha_1 = \alpha$ first. □

So, now we can define the trace and norm over $\mathbb{Q}$ in a nice way: given a number field $K$, we set

$$\operatorname{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \quad \text{and} \quad \operatorname{N}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

where $\sigma_i$ are the $n$ embeddings of $K$ into $\mathbb{C}$.

## §59.4 Everyone hates characteristic 2: separable vs irreducible

*Prototypical example for this section: $\mathbb{Q}$ has characteristic zero, hence irreducible polynomials are separable.*

Now, we want a version of the above theorem for any field $F$. If you read the proof, you'll see that the only thing that ever uses anything about the field $\mathbb{Q}$ is Lemma 54.1.2, where we use the fact that

> *Irreducible polynomials over $F$ have no double roots.*

Let's call a polynomial with no double roots **separable**; thus we want irreducible polynomials to be separable. We did this for $\mathbb{Q}$ in the last chapter by taking derivatives. Should work for any field, right?

Nope. Suppose we took the derivative of some polynomial like $2x^3 + 24x + 9$, namely $6x^2 + 24$. In $\mathbb{C}$ it's obvious that the derivative of a nonconstant polynomial $f'$ isn't zero. But suppose we considered the above as a polynomial in $\mathbb{F}_3$, i.e. modulo 3. Then the derivative is zero. Oh, no!

We have to impose a condition that prevents something like this from happening.

**Definition 59.4.1.** For a field $F$, the **characteristic** of $F$ is the smallest positive integer $p$ such that,

$$\underbrace{1_F + \cdots + 1_F}_{p \text{ times}} = 0$$

or zero if no such integer $p$ exists.

**Example 59.4.2** (Field characteristics)

Old friends $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ all have characteristic zero. But $\mathbb{F}_p$, the integers modulo $p$, is a field of characteristic $p$.

**Exercise 59.4.3.** Let $F$ be a field of characteristic $p$. Show that if $p > 0$ then $p$ is a prime number. (A proof is given next chapter.)

With the assumption of characteristic zero, our earlier proof works.

**Lemma 59.4.4** (Separability in characteristic zero)

Any irreducible polynomial in a characteristic zero field is separable.

Unfortunately, this lemma is false if the "characteristic zero" condition is dropped.

**Remark 59.4.5 —** The reason it's called *separable* is (I think) this picture: I have a polynomial and I want to break it into irreducible parts. Normally, if I have a double root in a polynomial, that means it's not irreducible. But in characteristic $p > 0$ this fails. So inseparable polynomials are strange when you think about them: somehow you have double roots that can't be separated from each other.

We can get this to work for any field extension in which separability is not an issue.

**Definition 59.4.6.** A **separable extension** $K/F$ is one where for each $\alpha \in K$, the minimal polynomial of $\alpha$ over $F$ is separable (for example, if $F$ has characteristic zero). A field $F$ is **perfect** if any finite field extension $K/F$ is separable.

In fact, as we see in the next chapter:

**Theorem 59.4.7** (Finite fields are perfect)

Suppose $F$ is a field with finitely many elements. Then it is perfect.

Thus, we will almost never have to worry about separability since every field we see in the Napkin is either finite or characteristic 0. So the inclusion of the word "separable" is mostly a formality.

Proceeding onwards, we obtain

**Theorem 59.4.8** (The $n$ embeddings of any separable extension)
Let $K/F$ be a separable extension of degree $n$ and let $\overline{F}$ be an algebraic closure of $F$. Then there are exactly $n$ field homomorphisms $K \hookrightarrow \overline{F}$, say $\sigma_1, \dots, \sigma_n$, which fix $F$.

In any case, this lets us define the trace for *any* separable normal extension.

**Definition 59.4.9.** Let $K/F$ be a separable extension of degree $n$, and let $\sigma_1, \dots, \sigma_n$ be the $n$ embeddings into an algebraic closure of $F$. Then we define

$$\mathrm{Tr}_{K/F}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \quad \text{and} \quad \mathrm{N}_{K/F}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

When $F = \mathbb{Q}$ and the algebraic closure is $\mathbb{C}$, this coincides with our earlier definition!

## §59.5 Automorphism groups and Galois extensions

*Prototypical example for this section:* $\mathbb{Q}(\sqrt{2})$ *is Galois but* $\mathbb{Q}(\sqrt[3]{2})$ *is not.*

We now want to get back at the idea we stated at the beginning of this section that $\mathbb{Q}(\sqrt[3]{2})$ is deficient in a way that $\mathbb{Q}(\sqrt{2})$ is not.

First, we define the "internal" automorphisms.

**Definition 59.5.1.** Suppose $K/F$ is a finite extension. Then $\mathrm{Aut}(K/F)$ is the set of *field isomorphisms* $\sigma \colon K \to K$ which fix $F$. In symbols

$$\mathrm{Aut}(K/F) = \{\sigma \colon K \to K \mid \sigma \text{ is identity on } F\}.$$

This is a group under function composition!

Note that this time, we have a condition that $F$ is fixed by $\sigma$. (This was not there before when we considered $F = \mathbb{Q}$, because we got it for free.)

**Example 59.5.2** (Old examples of automorphism groups)
Reprising the example at the beginning of the chapter in the new notation, we have:

(a) $\mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, with elements $z \mapsto z$ and $z \mapsto \overline{z}$.

(b) $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ in the same way.

(c) $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is the trivial group, with only the identity embedding!

**Example 59.5.3** (Automorphism group of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$)
Here's a new example: let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. It turns out that $\mathrm{Aut}(K/\mathbb{Q}) =$

$\{1, \sigma, \tau, \sigma\tau\}$, where

$$\sigma : \begin{cases} \sqrt{2} & \mapsto -\sqrt{2} \\ \sqrt{3} & \mapsto \sqrt{3} \end{cases} \quad \text{and} \quad \tau : \begin{cases} \sqrt{2} & \mapsto \sqrt{2} \\ \sqrt{3} & \mapsto -\sqrt{3}. \end{cases}$$

In other words, $\mathrm{Aut}(K/\mathbb{Q})$ is the Klein Four Group.

First, let's repeat the proof of the observation that these embeddings shuffle around roots (akin to the first observation in the introduction):

**Lemma 59.5.4** (Root shuffling in $\mathrm{Aut}(K/F)$)
Let $f \in F[x]$, suppose $K/F$ is a finite extension, and assume $\alpha \in K$ is a root of $f$. Then for any $\sigma \in \mathrm{Aut}(K/F)$, $\sigma(\alpha)$ is also a root of $f$.

*Proof.* Let $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$, where $c_i \in F$. Thus,

$$0 = \sigma(f(\alpha)) = \sigma\left(c_n\alpha^n + \cdots + c_0\right) = c_n\sigma(\alpha)^n + \cdots + c_0 = f(\sigma(\alpha)). \qquad \square$$

In particular, taking $f$ to be the minimal polynomial of $\alpha$ we deduce

**An embedding $\sigma \in \mathrm{Aut}(K/F)$ sends an $\alpha \in K$ to one of its various Galois conjugates (over $F$).**

Next, let's look again at the "deficiency" of certain fields. Look at $K = \mathbb{Q}(\sqrt[3]{2})$. So, again $K/\mathbb{Q}$ is deficient for two reasons. First, while there are three maps $\mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{C}$, only one of them lives in $\mathrm{Aut}(K/\mathbb{Q})$, namely the identity. In other words, $|\mathrm{Aut}(K/\mathbb{Q})|$ is *too small*. Secondly, $K$ is missing some Galois conjugates ($\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$).

The way to capture the fact that there are missing Galois conjugates is the notion of a splitting field.

**Definition 59.5.5.** Let $F$ be a field and $p(x) \in F[x]$ a polynomial of degree $n$. Then $p(x)$ has roots $\alpha_1, \ldots, \alpha_n$ in the algebraic closure of $F$. The **splitting field** of $p(x)$ over $F$ is defined as $F(\alpha_1, \ldots, \alpha_n)$.

In other words, the splitting field is the smallest field in which $p(x)$ splits.

**Example 59.5.6** (Examples of splitting fields)
(a) The splitting field of $x^2 - 5$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{5})$. This is a degree 2 extension.

(b) The splitting field of $x^2 + x + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\omega)$, where $\omega$ is a cube root of unity. This is a degree 2 extension.

(c) The splitting field of $x^2 + 3x + 2 = (x+1)(x+2)$ is just $\mathbb{Q}$! There's nothing to do.

**Example 59.5.7** (Splitting fields: a cautionary tale)
The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is in fact

$$\mathbb{Q}(\sqrt[3]{2}, \omega)$$

and not just $\mathbb{Q}(\sqrt[3]{2})$! One must really adjoin *all* the roots, and it's not necessarily

the case that these roots will generate each other.

To be clear:

- For $x^2-5$, we adjoin $\sqrt{5}$ and this will automatically include $-\sqrt{5}$.
- For $x^2+x+1$, we adjoin $\omega$ and get the other root $\omega^2$ for free.
- But for $x^3-2$, if we adjoin $\sqrt[3]{2}$, we do NOT get $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$ for free. Indeed, $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$!

Note that in particular, the splitting field of $x^3-2$ over $\mathbb{Q}$ is *degree six*, not just degree three.

In general, **the splitting field of a polynomial can be an extension of degree up to $n!$**. The reason is that if $p(x)$ has $n$ roots and no "coincidental" relations between them then any permutation of the roots will work.

Now, we obtain:

**Theorem 59.5.8** (Galois extensions are splitting)

For finite extensions $K/F$, $|\mathrm{Aut}(K/F)|$ divides $[K:F]$, with equality if and only if $K$ is the *splitting field* of some separable polynomial with coefficients in $F$.

The proof of this is deferred to an optional section at the end of the chapter. If $K/F$ is a finite extension and $|\mathrm{Aut}(K/F)| = [K:F]$, we say the extension $K/F$ is **Galois**. In that case, we denote $\mathrm{Aut}(K/F)$ by $\mathrm{Gal}(K/F)$ instead and call this the **Galois group** of $K/F$.

**Example 59.5.9** (Examples and non-examples of Galois extensions)

(a) The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois, since it's the splitting field of $x^2-2$ over $\mathbb{Q}$. The Galois group has order two, $\sqrt{2} \mapsto \pm\sqrt{2}$.

(b) The extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is Galois, since it's the splitting field of $(x^2-5)^2-6$ over $\mathbb{Q}$. As discussed before, the Galois group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(c) The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is *not* Galois.

To explore $\mathbb{Q}(\sqrt[3]{2})$ one last time:

**Example 59.5.10** (Galois closures, and the automorphism group of $\mathbb{Q}(\sqrt[3]{2},\omega)$)

Let's return to the field $K = \mathbb{Q}(\sqrt[3]{2},\omega)$, which is a field with $[K:\mathbb{Q}] = 6$. Consider the two automorphisms:

$$\sigma : \begin{cases} \sqrt[3]{2} & \mapsto \omega\sqrt[3]{2} \\ \omega & \mapsto \omega \end{cases} \quad \text{and} \quad \tau : \begin{cases} \sqrt[3]{2} & \mapsto \sqrt[3]{2} \\ \omega & \mapsto \omega^2. \end{cases}$$

Notice that $\sigma^3 = \tau^2 = \mathrm{id}$. From this one can see that the automorphism group of $K$ must have order 6 (it certainly has order $\le 6$; now use Lagrange's theorem). So, $K/\mathbb{Q}$ is Galois! Actually one can check explicitly that

$$\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$$

is the symmetric group on 3 elements, with order $3! = 6$.

This example illustrates the fact that given a non-Galois field extension, one can "add in" missing conjugates to make it Galois. This is called taking a **Galois closure**.

## §59.6 Fundamental theorem of Galois theory

After all this stuff about Galois Theory, I might as well tell you the fundamental theorem, though I won't prove it. Basically, it says that if $K/F$ is Galois with Galois group $G$, then:

**Subgroups of $G$ correspond exactly to fields $E$ with $F \subseteq E \subseteq K$.**

To tell you how the bijection goes, I have to define a fixed field.

**Definition 59.6.1.** Let $K$ be a field and $H$ a subgroup of $\text{Aut}(K/F)$. We define the **fixed field** of $H$, denoted $K^H$, as

$$K^H := \{x \in K : \sigma(x) = x \ \forall \sigma \in H\}.$$

**Question 59.6.2.** Verify quickly that $K^H$ is actually a field.

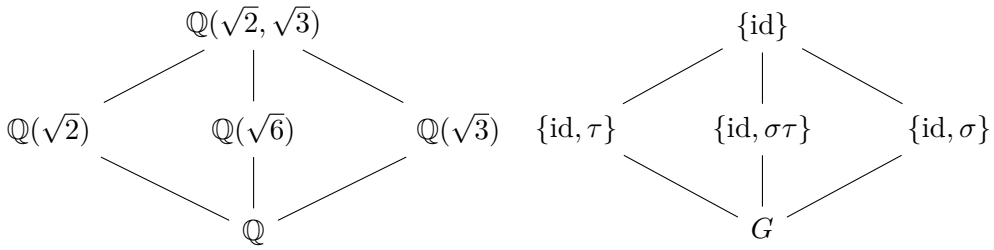
Now let's look at examples again. Consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, where

$$G = \text{Gal}(K/\mathbb{Q}) = \{\text{id}, \sigma, \tau, \sigma\tau\}$$

is the Klein four group (where $\sigma(\sqrt{2}) = -\sqrt{2}$ but $\sigma(\sqrt{3}) = \sqrt{3}$; $\tau$ goes the other way).

**Question 59.6.3.** Let $H = \{\text{id}, \sigma\}$. What is $K^H$?

In that case, the diagram of fields between $\mathbb{Q}$ and $K$ matches exactly with the subgroups of $G$, as follows:




We see that subgroups correspond to fixed fields. That, and much more, holds in general.

**Theorem 59.6.4** (Fundamental theorem of Galois theory)
Let $K/F$ be a Galois extension with Galois group $G = \text{Gal}(K/F)$.

(a) There is a bijection between field towers $F \subseteq E \subseteq K$ and subgroups $H \subseteq G$:

$$\left\{ \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \iff \left\{ \begin{array}{c} 1 \\ | \\ H \\ | \\ G \end{array} \right\}$$

The bijection sends $H$ to its fixed field $K^H$, and hence is inclusion reversing.

(b) Under this bijection, we have $[K : E] = |H|$ and $[E : F] = |G/H|$.

(c) $K/E$ is always Galois, and its Galois group is $\text{Gal}(K/E) = H$.

(d) $E/F$ is Galois if and only if $H$ is normal in $G$. If so, $\text{Gal}(E/F) = G/H$.

**Exercise 59.6.5.** Suppose we apply this theorem for

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega).$$

Verify that the fact $E = \mathbb{Q}(\sqrt[3]{2})$ is not Galois corresponds to the fact that $S_3$ does not have normal subgroups of order 2.

## §59.7 A few harder problems to think about

**Problem 59A**$^\star$ (Galois group of the cyclotomic field)**.** Let $p$ be an odd rational prime and $\zeta_p$ a primitive $p$th root of unity. Let $K = \mathbb{Q}(\zeta_p)$. Show that

$$\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times.$$

**Problem 59B.** Give an example of a degree-three Galois extension of $\mathbb{Q}$.

**Problem 59C** (Greek constructions)**.** Prove that the three Greek constructions

(a) doubling the cube,

(b) squaring the circle, and

(c) trisecting an angle

are all impossible. (Assume $\pi$ is transcendental.)

**Problem 59D** (China Hong Kong Math Olympiad)**.** Prove that there are no rational numbers $p$, $q$, $r$ satisfying

$$\cos\left(\frac{2\pi}{7}\right) = p + \sqrt{q} + \sqrt[3]{r}.$$

**Problem 59E.** Show that the only automorphism of $\mathbb{R}$ is the identity. Hence $\text{Aut}(\mathbb{R}/\mathbb{Q})$ is the trivial group.

**Problem 59F** (Artin's primitive element theorem)**.** Let $K$ be a number field. Show that $K \cong \mathbb{Q}(\gamma)$ for some $\gamma$.

## §59.8 (Optional) Proof that Galois extensions are splitting

We prove Theorem 59.5.8. First, we extract a useful fragment from the fundamental theorem.

**Theorem 59.8.1** (Fixed field theorem)
Let $K$ be a field and $G$ a subgroup of $\operatorname{Aut}(K)$. Then $[K : K^G] = |G|$.

The inequality itself is not difficult:

**Exercise 59.8.2.** Show that $[K : F] \geq |\operatorname{Aut}(K/F)|$, and that equality holds if and only if the set of elements fixed by all $\sigma \in \operatorname{Aut}(K/F)$ is exactly $F$. (Use Theorem 59.8.1.)

The equality case is trickier.

The easier direction is when $K$ is a splitting field. Assume $K = F(\alpha_1, \dots, \alpha_n)$ is the splitting field of some separable polynomial $p \in F[x]$ with $n$ distinct roots $\alpha_1, \dots, \alpha_n$. Adjoin them one by one:

$$\begin{array}{ccccccccc}
F & \hookrightarrow & F(\alpha_1) & \hookrightarrow & F(\alpha_1,\alpha_2) & \hookrightarrow & \dots & \hookrightarrow & K \\
\downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \tau_1} & & \downarrow{\scriptstyle \tau_2} & & & & \downarrow{\scriptstyle \tau_n=\sigma} \\
F & \hookrightarrow & F(\alpha_1) & \hookrightarrow & F(\alpha_1,\alpha_2) & \hookrightarrow & \dots & \hookrightarrow & K
\end{array}$$

(Does this diagram look familiar?) Every map $K \to K$ which fixes $F$ corresponds to an above commutative diagram. As before, there are exactly $[F(\alpha_1) : F]$ ways to pick $\tau_1$. (You need the fact that the minimal polynomial $p_1$ of $\alpha_1$ is separable for this: there need to be exactly $\deg p_1 = [F(\alpha_1) : F]$ distinct roots to nail $p_1$ into.) Similarly, given a choice of $\tau_1$, there are $[F(\alpha_1, \alpha_2) : F(\alpha_1)]$ ways to pick $\tau_2$. Multiplying these all together gives the desired $[K : F]$.

Now assume $K/F$ is Galois. First, we state:

**Lemma 59.8.3**
Let $K/F$ be Galois, and $p \in F[x]$ irreducible. If any root of $p$ (in $\overline{F}$) lies in $K$, then all of them do, and in fact $p$ is separable.

*Proof.* Let $\alpha \in K$ be the prescribed root. Consider the set

$$S = \{\sigma(\alpha) \mid \sigma \in \operatorname{Gal}(K/F)\}.$$

(Note that $\alpha \in S$ since $\operatorname{Gal}(K/F) \ni \mathrm{id}$.) By construction, any $\tau \in \operatorname{Gal}(K/F)$ fixes $S$. So if we construct

$$\tilde{p}(x) = \prod_{\beta \in S} (x - \beta),$$

then by Vieta's Formulas, we find that all the coefficients of $\tilde{p}$ are fixed by elements of $\sigma$. By the *equality case* we specified in the exercise, it follows that $\tilde{p}$ has coefficients in $F$! (This is where we use the condition.) Also, by Lemma 59.5.4, $\tilde{p}$ divides $p$.

Yet $p$ was irreducible, so it is the minimal polynomial of $\alpha$ in $F[x]$, and therefore we must have that $p$ divides $\tilde{p}$. Hence $p = \tilde{p}$. Since $\tilde{p}$ was built to be separable, so is $p$. □

Now we're basically done – pick a basis $\omega_1, \dots, \omega_n$ of $K/F$, and let $p_i$ be their minimal polynomials; by the above, we don't get any roots outside $K$. Consider $P = p_1 \dots p_n$, removing any repeated factors. The roots of $P$ are $\omega_1, \dots, \omega_n$ and some other guys in $K$. So $K$ is the splitting field of $P$.

# 60 Finite fields

In this short chapter, we classify all fields with finitely many elements and compute the Galois groups. Nothing in here is very hard, and so most of the proofs are just sketches; if you like, you should check the details yourself.

The whole point of this chapter is to prove:

- A finite field $F$ must have order $p^n$, with $p$ prime and $n$ an integer.
- In this case, $F$ has characteristic $p$.
- All such fields are isomorphic, so it's customary to use the notation $\mathbb{F}_{p^n}$ for "the" finite field of order $p^n$ if we only care up to isomorphism.
- The extension $F/\mathbb{F}_p$ is Galois, and $\mathrm{Gal}(F/\mathbb{F}_p)$ is a cyclic group of order $n$. The generator is the automorphism

$$\sigma \colon F \to F \quad \text{by} \quad x \mapsto x^p.$$

If you're in a hurry you can just remember these results and skip to the next chapter.

## §60.1 Example of a finite field

Before diving in, we give some examples.

Recall that the *characteristic* of a field $F$ is the smallest positive integer $p$ such that

$$\underbrace{1_F + \cdots + 1_F}_{p \text{ times}} = 0$$

or 0 if no such integer $p$ exists.

**Example 60.1.1** (Base field)

Let $\mathbb{F}_p$ denote the field of integers modulo $p$. This is a field with $p$ elements, with characteristic $p$.

**Example 60.1.2** (The finite field of nine elements)

Let

$$F \cong \mathbb{F}_3[X]/(X^2+1) \cong \mathbb{Z}[i]/(3).$$

We can think of its elements as

$$\{a + bi \mid 0 \le a, b \le 2\}.$$

Since (3) is prime in $\mathbb{Z}[i]$, the ring of integers of $\mathbb{Q}(i)$, we see $F$ is a field with $3^2 = 9$ elements inside it. Note that, although this field has 9 elements, every element $x$ has

the property that

$$3x = \underbrace{x + \cdots + x}_{3 \text{ times}} = 0.$$

In particular, $F$ has characteristic 3.

## §60.2 Finite fields have prime power order

**Lemma 60.2.1**

If the characteristic of a field $F$ isn't zero, it must be a prime number.

*Proof.* Assume not, so $n = ab$ for $a, b < n$. Then let

$$A = \underbrace{1_F + \cdots + 1_F}_{a \text{ times}} \neq 0$$

and

$$B = \underbrace{1_F + \cdots + 1_F}_{b \text{ times}} \neq 0.$$

Then $AB = 0$, contradicting the fact that $F$ is a field. □

We like fields of characteristic zero, but unfortunately for finite fields we are doomed to have nonzero characteristic.

**Lemma 60.2.2** (Finite fields have prime power orders)

Let $F$ be a finite field. Then

(a) Its characteristic is nonzero, and hence some prime $p$.

(b) The field $F$ is a finite extension of $\mathbb{F}_p$, and in particular it is an $\mathbb{F}_p$-vector space.

(c) We have $|F| = p^n$ for some prime $p$, integer $n$.

*Proof.* Very briefly, since this is easy:

(a) Apply Lagrange's theorem (or pigeonhole principle!) to $(F, +)$ to get the characteristic isn't zero.

(b) The additive subgroup of $(F, +)$ generated by $1_F$ is an isomorphic copy of $\mathbb{F}_p$.

(c) Since it's a field extension, $F$ is a finite-dimensional vector space over $\mathbb{F}_p$, with some basis $e_1, \ldots, e_n$. It follows that there are $p^n$ elements of $F$. □

**Remark 60.2.3 —** An amusing alternate proof of (c) by contradiction: if a prime $q \neq p$ divides $|F|$, then by Cauchy's theorem (Problem 17A⋆) on $(F, +)$ there's a (nonzero) element $x$ of order $q$. Evidently

$$x \cdot (\underbrace{1_F + \cdots + 1_F}_{q \text{ times}}) = 0$$

then, but $x \neq 0$, and hence the characteristic of $F$ also divides $q$, which is impossible.

An important point in the above proof is that

**Lemma 60.2.4** (Finite fields are field extensions of $\mathbb{F}_p$)
If $|F| = p^n$ is a finite field, then there is an isomorphic copy of $\mathbb{F}_p$ sitting inside $F$. Thus $F$ is a field extension of $\mathbb{F}_p$.

We want to refer a lot to this copy of $\mathbb{F}_p$, so in what follows:

**Abuse of Notation 60.2.5.** Every integer $n$ can be identified as an element of $F$, namely

$$n \coloneqq \underbrace{1_F + \cdots + 1_F}_{n \text{ times}}.$$

Note that (as expected) this depends only on $n \pmod p$.

This notation makes it easier to think about statements like the following.

**Theorem 60.2.6** (Freshman's dream)
For any $a, b \in F$ we have

$$(a+b)^p = a^p + b^p.$$

*Proof.* Use the Binomial theorem, and the fact that $\binom{p}{i}$ is divisible by $p$ for $0 < i < p$. □

**Exercise 60.2.7.** Convince yourself that this proof works.

## §60.3 All finite fields are isomorphic

We next proceed to prove "Fermat's little theorem":

**Theorem 60.3.1** (Fermat's little theorem in finite fields)
Let $F$ be a finite field of order $p^n$. Then every element $x \in F$ satisfies

$$x^{p^n} - x = 0.$$

*Proof.* If $x = 0$ it's true; otherwise, use Lagrange's theorem on the abelian group $(F, \times)$ to get $x^{p^n - 1} = 1_F$. □

We can now prove the following result, which is the "main surprise" about finite fields: that there is a unique one up to isomorphism for each size.

**Theorem 60.3.2** (Complete classification of finite fields)
A field $F$ is a finite field with $p^n$ elements if and only if it is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

*Proof.* By "Fermat's little theorem", all the elements of $F$ satisfy this polynomial. So we just have to show that the roots of this polynomial are distinct (i.e. that it is separable).

To do this, we use the derivative trick again: the derivative of this polynomial is

$$p^n \cdot x^{p^n-1} - 1 = -1$$

which has no roots at all, so the polynomial cannot have any double roots. □

**Definition 60.3.3.** For this reason, it's customary to denote *the* field with $p^n$ elements by $\mathbb{F}_{p^n}$.

Note that the polynomial $x^{p^n} - x \pmod p$ is far from irreducible, but the computation above shows that it's separable.

**Example 60.3.4** (The finite field of order nine again)

The polynomial $x^9 - x$ is separable modulo 3 and has factorization

$$x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2) \pmod 3.$$

So if $F$ has order 9, then we intuitively expect it to be the field generated by adjoining all the roots: 0, 1, 2, as well as $\pm i$, $1 \pm i$, $2 \pm i$. Indeed, that's the example we had at the beginning of this chapter.

(Here $i$ denotes *an* element of $\mathbb{F}_9$ satisfying $i^2 = -1$. The notation is deliberately similar to the usual imaginary unit.)

## §60.4 The Galois theory of finite fields

Retain the notation $\mathbb{F}_{p^n}$ now (instead of $F$ like before). By the above theorem, it's the splitting field of a separable polynomial, hence we know that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension. We would like to find the Galois group.

In fact, we are very lucky: it is cyclic. First, we exhibit one such element $\sigma_p \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$:

**Theorem 60.4.1** (The $p$th power automorphism)

The map $\sigma_p \colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ defined by

$$\sigma_p(x) = x^p$$

is an automorphism, and moreover fixes $\mathbb{F}_p$.

This is called the Frobenius automorphism, and will re-appear later on in Chapter 62.

*Proof.* It's a homomorphism since it fixes 1, respects multiplication, and respects addition.

> **Question 60.4.2.** Why does it respect addition?

Next, we claim that it is injective. To see this, note that

$$x^p = y^p \iff x^p - y^p = 0 \iff (x-y)^p = 0 \iff x = y.$$

Here we have again used the Freshman's Dream. Since $\mathbb{F}_{p^n}$ is finite, this injective map is automatically bijective. The fact that it fixes $\mathbb{F}_p$ is Fermat's little theorem. □

Now we're done:

**Theorem 60.4.3** (Galois group of the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$)
We have $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ with generator $\sigma_p$.

*Proof.* Since $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, the Galois group $G$ has order $n$. So we just need to show $\sigma_p \in G$ has order $n$.

Note that $\sigma_p$ applied $k$ times gives $x \mapsto x^{p^k}$. Hence, $\sigma_p$ applied $n$ times is the identity, as all elements of $\mathbb{F}_{p^n}$ satisfy $x^{p^n} = x$. But if $k < n$, then $\sigma_p$ applied $k$ times cannot be the identity or $x^{p^k} - x$ would have too many roots. □

We can see an example of this again with the finite field of order 9.

**Example 60.4.4** (Galois group of finite field of order 9)
Let $\mathbb{F}_9$ be the finite field of order 9, and represent it concretely by $\mathbb{F}_9 = \mathbb{Z}[i]/(3)$. Let $\sigma_3 \colon \mathbb{F}_9 \to \mathbb{F}_9$ be $x \mapsto x^3$. We can witness the fate of all nine elements:

$$\begin{array}{ccccccc} 0 & & 1 & & 2 & & i \\ & & & & & & \updownarrow \sigma \\ & & & & & & -i \end{array} \qquad \begin{array}{ccc} 1+i & & 2+i \\ \updownarrow \sigma & & \updownarrow \sigma \\ 1-i & & 2-i \end{array}$$

(As claimed, 0, 1, 2 are the fixed points, so I haven't drawn arrows for them.) As predicted, the Galois group has order two:

$$\mathrm{Gal}(\mathbb{F}_9/\mathbb{F}_3) = \{\mathrm{id}, \sigma_3\} \cong \mathbb{Z}/2\mathbb{Z}.$$

This concludes the proof of all results stated at the beginning of this chapter.

## §60.5 Extra: The multiplicative group of a finite field

In this section we prove a result which is interesting by its own right, even though it is not used in the following chapters.

Consider the field $F$ of order $p = 17$. We may want to ask the following questions about $F$:

- How many nonzero elements in $F$ is a quadratic residue (can be written as a square of another element in $F$)?
- Is there any element $x$ in $p$ such that $x^2 = -1$?

With the following proposition, the questions above become easy.

**Proposition 60.5.1**
Let $F$ be a finite field, then the multiplicative group $F^\times$ is a cyclic group.

Essentially, it says that the multiplicative group $F^\times$ is as nice as possible — the cyclic group is the simplest Abelian group!

If we look back at the examples above, we can see how this knowledge can help us.

**Example 60.5.2** (The multiplicative group of $\mathbb{F}_{17}$)

The group $F^\times$ is cyclic of order 16, so there is some element $g \in F^\times$ such that all of the elements in $F$ are

$$0, g^0 = 1, g^1, g^2, \dots, g^{15}.$$

Using this knowledge, if we square the nonzero elements, we can easily see that the result are the following (note that $g^{16} = g^0 = 1$):

$$g^0, g^2, g^4, \dots, g^{14}, g^0, g^2, \dots, g^{14}.$$

As such, exactly half of the elements — 8 elements — in $F^\times$ are quadratic residues!

Checking whether there is an element $x$ such that $x^2 = -1$ isn't much harder. First, where may $-1$ appear in the sequence $\{g^0, g^1, \dots, g^{15}\}$? If you find an explicit value of $g$ (you can pick $g = 3$ for instance), you will see that $g^8 = -1$. But, even without an explicit calculation, you can still see that, because:

> **Question 60.5.3.** Note that the equation $x^2 = 1$ has only 2 roots, 1 and $-1$. Using group operations in the group $F^\times$, what does the equation say?

We have $g^8 = -1$, so $(g^4)^2 = (g^{12})^2 = -1$, so we're done.

So, why is the proposition true? Consider a finite field $F$ of order a prime power $q$. First, using an idea similar to the above, we have:

> **Question 60.5.4.** Show that, for any positive $d < |F^\times| = q - 1$, then there are at most $d$ elements $x$ such that $x^d = 1$.

The rest is easily handled using group theory. Recall from Theorem 18.1.5, because $F^\times$ is a finite Abelian group, it is in particular finitely generated, and can be written in the form

$$F^\times \cong \mathbb{Z}^{\oplus r} \oplus \mathbb{Z}/q_1\mathbb{Z} \oplus \mathbb{Z}/q_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_m\mathbb{Z}.$$

Of course, $r = 0$ here.

Now, assume $F^\times$ is not cyclic, so the lowest common denominator of all the $q_i$ values are less than $|F^\times|$. Then, for all $x \in F^\times$, $x^{\operatorname{lcm}(q_1,\dots,q_m)} = 1$, which gives a contradiction.

> **Remark 60.5.5 —** If you look up an elementary proof of why there are exactly $p - 1$ quadratic residues modulo $p$, most of the time, you will get some argument using "$x^d - 1$ has at most $d$ roots" similar to the proof above, but by not going all the way and show the structure of the multiplicative group, it hides the spirit of what is really going on.
>
> The proposition above takes a step further — now, without any calculation, you know for instance the finite field $\mathbb{F}_{17^2}$ has exactly $\frac{17^2-1}{2} = 144$ nonzero quadratic residues.

## §60.6 A few harder problems to think about

**Problem 60A**$^\dagger$ (HMMT 2017)**.** What is the period of the Fibonacci sequence modulo 127?

# 61 Ramification theory

We're very interested in how rational primes $p$ factor in a bigger number field $K$. Some examples of this behavior: in $\mathbb{Z}[i]$ (which is a UFD!), we have factorizations

$$\begin{aligned}(2) &= (1+i)^2 \\ (3) &= (3) \\ (5) &= (2+i)(2-i).\end{aligned}$$

In this chapter we'll learn more about how primes break down when they're thrown into bigger number fields. Using weapons from Galois Theory, this will culminate in a proof of Quadratic Reciprocity.

## §61.1 Ramified / inert / split primes

*Prototypical example for this section: In $\mathbb{Z}[i]$, 2 is ramified, 3 is inert, and 5 splits.*

Let $p$ be a rational prime, and toss it into $\mathcal{O}_K$. Thus we get a factorization into prime ideals

$$p \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}.$$

We say that each $\mathfrak{p}_i$ is **above** $(p)$.[1] Pictorially, you might draw this as follows:

$$\begin{array}{ccccc} K & \supset & \mathcal{O}_K & & \mathfrak{p}_i \\ | & & | & & | \\ \mathbb{Q} & \supset & \mathbb{Z} & & (p) \end{array}$$

Some names for various behavior that can happen:

- We say $p$ is **ramified** if $e_i > 1$ for some $i$. For example 2 is ramified in $\mathbb{Z}[i]$.
- We say $p$ is **inert** if $g = 1$ and $e_1 = 1$; i.e. $(p)$ remains prime. For example 3 is inert in $\mathbb{Z}[i]$.
- We say $p$ is **split** if $g > 1$. For example 5 is split in $\mathbb{Z}[i]$.

**Question 61.1.1.** More generally, for a prime $p$ in $\mathbb{Z}[i]$:

- $p$ is ramified exactly when $p = 2$.
- $p$ is inert exactly when $p \equiv 3 \pmod 4$.
- $p$ is split exactly when $p \equiv 1 \pmod 4$.

Prove this.

[1] Reminder that $p \cdot \mathcal{O}_K$ and $(p)$ mean the same thing, and I'll use both interchangeably.

## §61.2 Primes ramify if and only if they divide $\Delta_K$

The most unusual case is ramification: Just like we don't expect a randomly selected polynomial to have a double root, we don't expect a randomly selected prime to be ramified. In fact, the key to understanding ramification is the discriminant.

For the sake of discussion, let's suppose that $K$ is monogenic, $\mathcal{O}_K = \mathbb{Z}[\theta]$, where $\theta$ has minimal polynomial $f$. Let $p$ be a rational prime we'd like to factor. If $f$ factors as $f_1^{e_1} \dots f_g^{e_g}$, then we know that the prime factorization of $(p)$ is given by

$$p \cdot \mathcal{O}_K = \prod_i (p, f_i(\theta))^{e_i}.$$

In particular, $p$ ramifies exactly when $f$ *has a double root mod* $p$! To detect whether this happens, we look at the polynomial discriminant of $f$, namely

$$\Delta(f) = \prod_{i<j} (z_i - z_j)^2$$

and see whether it is zero mod $p$ – thus $p$ ramifies if and only if this is true.

It turns out that the naïve generalization to any number field works if we replace $\Delta(f)$ by just the discriminant $\Delta_K$ of $K$; (these are the same for monogenic $\mathcal{O}_K$ by Problem 57C$^\star$). That is,

**Theorem 61.2.1** (Discriminant detects ramification)
Let $p$ be a rational prime and $K$ a number field. Then $p$ is ramified if and only if $p$ divides $\Delta_K$.

**Example 61.2.2** (Ramification in the Gaussian integers)
Let $K = \mathbb{Q}(i)$ so $\mathcal{O}_K = \mathbb{Z}[i]$ and $\Delta_K = -4$. As predicted, the only prime ramifying in $\mathbb{Z}[i]$ is 2, the only prime factor of $\Delta_K$.

In particular, only finitely many primes ramify.

## §61.3 Inertial degrees

*Prototypical example for this section:* $(7)$ *has inertial degree* 2 *in* $\mathbb{Z}[i]$ *and* $(2+i)$ *has inertial degree* 1 *in* $\mathbb{Z}[i]$.

Recall that we were able to define an ideal norm $\mathrm{N}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ measuring how "roomy" the ideal $\mathfrak{a}$ is. For example, $(5)$ has ideal norm $5^2 = 25$ in $\mathbb{Z}[i]$, since

$$\mathbb{Z}[i]/(5) \cong \{a + bi \mid a, b \in \mathbb{Z}/5\mathbb{Z}\}$$

has $5^2 = 25$ elements.

Now, let's look at

$$p \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$$

in $\mathcal{O}_K$, where $K$ has degree $n$. Taking the ideal norms of both sides, we have that

$$p^n = \mathrm{N}(\mathfrak{p}_1)^{e_1} \dots \mathrm{N}(\mathfrak{p}_g)^{e_g}.$$

We conclude that $\mathrm{N}(\mathfrak{p}_i) = p^{f_i}$ for some integer $f_i \geq 1$, and moreover that

$$n = \sum_{i=1}^{g} e_i f_i.$$

**Definition 61.3.1.** We say $f_i$ is the **inertial degree** of $\mathfrak{p}_i$, and $e_i$ is the **ramification index**.

**Example 61.3.2** (Examples of inertial degrees)

Work in $\mathbb{Z}[i]$, which is degree 2. The inertial degree detects how "spacy" the given $\mathfrak{p}$ is when interpreted in $\mathcal{O}_K$.

(a) The prime $7 \cdot \mathbb{Z}[i]$ has inertial degree 2. Indeed, $\mathbb{Z}[i]/(7)$ has $7^2 = 49$ elements, those of the form $a + bi$ for $a$, $b$ modulo 7. It gives "two degrees" of space.

(b) Let $(5) = (2+i)(2-i)$. The inertial degrees of $(2+i)$ and $(2-i)$ are both 1. Indeed, $\mathbb{Z}[i]/(2+i)$ only gives "one degree" of space, since each of its elements can be viewed as integers modulo 5, and there are only $5^1 = 5$ elements.

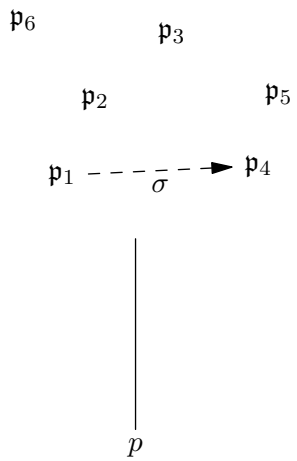
If you understand this, it should be intuitively clear why the sum of $e_i f_i$ should equal $n$.

## §61.4 The magic of Galois extensions

OK, that's all fine and well. But something *really magical* happens when we add the additional hypothesis that $K/\mathbb{Q}$ is *Galois*: all the inertial degrees and ramification indices are equal. We set about proving this.

Let $K/\mathbb{Q}$ be Galois with $G = \mathrm{Gal}(K/\mathbb{Q})$. Note that if $\mathfrak{p} \subseteq \mathcal{O}_K$ is a prime above $p$, then the image $\sigma^{\mathrm{img}}(\mathfrak{p})$ is also prime for any $\sigma \in G$ (since $\sigma$ is an automorphism!). Moreover, since $p \in \mathfrak{p}$ and $\sigma$ fixes $\mathbb{Q}$, we know that $p \in \sigma^{\mathrm{img}}(\mathfrak{p})$ as well.

Thus, by the pointwise mapping, **the Galois group acts on the prime ideals above a rational prime** $p$. Picture:




The notation $\sigma^{\mathrm{img}}(\mathfrak{p})$ is hideous in this context, since we're really thinking of $\sigma$ as just doing a group action, and so we give the shorthand:

**Abuse of Notation 61.4.1.** Let $\sigma\mathfrak{p}$ be shorthand for $\sigma^{\text{img}}(\mathfrak{p})$.

Since the $\sigma$'s are all bijections (they are automorphisms!), it should come as no surprise that the prime ideals which are in the same orbit are closely related. But miraculously, it turns out there is only one orbit!

**Theorem 61.4.2** (Galois group acts transitively)
Let $K/\mathbb{Q}$ be Galois with $G = \text{Gal}(K/\mathbb{Q})$. Let $\{\mathfrak{p}_i\}$ be the set of distinct prime ideals in the factorization of $p \cdot \mathcal{O}_K$ (in $\mathcal{O}_K$).

Then $G$ acts transitively on the $\mathfrak{p}_i$: for every $i$ and $j$, we can find $\sigma$ such that $\sigma\mathfrak{p}_i = \mathfrak{p}_j$.

In other words,

**All of the $\{\mathfrak{p}_i\}$ are Galois conjugates of each other.**

Before proving this, let us consider the easier problem of factorization into elements.

> Suppose $\mathcal{O}_K$ is an UFD, and $p$ factors as $up_1p_2\cdots p_n$ in $\mathcal{O}_K$, where $p_i$ are irreducibles and $u$ is an unit. Show that the $p_i$ are all conjugates of each other, up to multiplication by an unit.

**Question 61.4.3.** Try to prove it before reading it below. (Hint: Galois theory. Alternatively, take the norm of $p_1$.)

*Proof.* Let $q = \text{N}_{K/\mathbb{Q}}(p_1)$ be the product of all conjugates of $p_1$, then $q \in \mathbb{Q}$. Thus $p \mid q$, so each $p_i$ is a factor of $q$, and we're done by unique factorization. □

Unfortunately, the product of all conjugates of an ideal $\mathfrak{p}_1$ is not necessarily of the form $p \cdot \mathcal{O}_K$ (for example, $K = \mathbb{Q}[i]$ and $(1+i)$ has no other conjugates). So in the proof, we pick $x$ which is an "representative" of $\mathfrak{p}_1$.

*Proof of Theorem 61.4.2.* Because $\mathfrak{p}_i$ are distinct primes, by the Chinese remainder theorem, we can find an $x \in \mathcal{O}_K$ such that

$$\begin{aligned} x &\equiv 0 \pmod{\mathfrak{p}_1} \\ x &\equiv 1 \pmod{\mathfrak{p}_i} \text{ for } i \geq 2 \end{aligned}$$

Then, compute the norm

$$\text{N}_{K/\mathbb{Q}}(x) = \prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} \sigma(x).$$

Each $\sigma(x)$ is in $K$ because $K/\mathbb{Q}$ is Galois!

Since $\text{N}_{K/\mathbb{Q}}(x)$ is an integer and divisible by $\mathfrak{p}_1$, we should have that $\text{N}_{K/\mathbb{Q}}(x)$ is divisible by $p$. Thus it should be divisible by $\mathfrak{p}_2$ as well. Thus, for some $\sigma \in \text{Gal}(K/\mathbb{Q})$, $\sigma(x)$ is divisible by $\mathfrak{p}_2$, equivalently, $x$ is divisible by $\sigma^{-1}\mathfrak{p}_2$. But by the way we selected $x$, we have within the factors of $p$, $x$ is divisible by only $\mathfrak{p}_1$! So $\sigma^{-1}\mathfrak{p}_2 = \mathfrak{p}_1$, and we're done. □

**Theorem 61.4.4** (Inertial degree and ramification indices are all equal)
Assume $K/\mathbb{Q}$ is Galois. Then for any rational prime $p$ we have

$$p \cdot \mathcal{O}_K = (\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_g)^e$$

for some $e$, where the $\mathfrak{p}_i$ are distinct prime ideals with the same inertial degree $f$. Hence

$$[K : \mathbb{Q}] = efg.$$

*Proof.* To see that the inertial degrees are equal, note that each $\sigma$ induces an isomorphism

$$\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_K/\sigma(\mathfrak{p}).$$

Because the action is transitive, all $f_i$ are equal.

**Exercise 61.4.5.** Using the fact that $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, show that

$$\sigma^{\mathrm{img}}(p \cdot \mathcal{O}_K) = p \cdot \sigma^{\mathrm{img}}(\mathcal{O}_K) = p \cdot \mathcal{O}_K.$$

So for every $\sigma$, we have that $p \cdot \mathcal{O}_K = \prod \mathfrak{p}_i^{e_i} = \prod(\sigma\mathfrak{p}_i)^{e_i}$. Since the action is transitive, all $e_i$ are equal. □

Let's see an illustration of this.

**Example 61.4.6** (Factoring 5 in a Galois/non-Galois extension)
Let $p = 5$ be a prime.

(a) Let $E = \mathbb{Q}(\sqrt[3]{2})$. One can show that $\mathcal{O}_E = \mathbb{Z}[\sqrt[3]{2}]$, so we use the Factoring Algorithm on the minimal polynomial $x^3 - 2$. Since $x^3 - 2 \equiv (x-3)(x^2+3x+9) \pmod 5$ is the irreducible factorization, we have that

$$(5) = (5, \sqrt[3]{2} - 3)(5, \sqrt[3]{4} + 3\sqrt[3]{2} + 9)$$

which have inertial degrees 1 and 2, respectively. The fact that this is not uniform reflects that $E$ is not Galois.

(b) Now let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$, which is the splitting field of $x^3 - 2$ over $\mathbb{Q}$; now $K$ is Galois. It turns out that

$$\mathcal{O}_K = \mathbb{Z}[\varepsilon] \quad \text{where} \quad \varepsilon \text{ is a root of } t^6 + 3t^5 - 5t^3 + 3t + 1.$$

(this takes a lot of work to obtain, so we won't do it here). Modulo 5 this has an irreducible factorization $(x^2+x+2)(x^2+3x+3)(x^2+4x+1) \pmod 5$, so by the Factorization Algorithm,

$$(5) = (5, \varepsilon^2 + \varepsilon + 2)(5, \varepsilon^2 + 3\varepsilon + 3)(5, \varepsilon^2 + 4\varepsilon + 1).$$

This time all inertial degrees are 2, as the theorem predicts for $K$ Galois.

## §61.5 (Optional) Decomposition and inertia groups

Let $p$ be a rational prime. Thus

$$p \cdot \mathcal{O}_K = (\mathfrak{p}_1 \dots \mathfrak{p}_g)^e$$

and all the $\mathfrak{p}_i$ have inertial degree $f$. Let $\mathfrak{p}$ denote a choice of the $\mathfrak{p}_i$.

We can look at both the fields $\mathcal{O}_K/\mathfrak{p}$ and $\mathbb{Z}/p = \mathbb{F}_p$. Naturally, since $\mathcal{O}_K/\mathfrak{p}$ is a finite field we can view it as a field extension of $\mathbb{F}_p$. So we can get the diagram

$$\begin{array}{ccccc} K & \supset & \mathcal{O}_K & \mathfrak{p} & \mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f} \\ | & & | & | & | \\ \mathbb{Q} & \supset & \mathbb{Z} & (p) & \mathbb{F}_p. \end{array}$$

At the far right we have finite field extensions, which we know are *really* well behaved. So we ask:

> *How are* $\mathrm{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right)$ *and* $\mathrm{Gal}(K/\mathbb{Q})$ *related?*

First, every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ induces an automorphism of $\mathcal{O}_K$, which induces a map $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$ by

$$\alpha \mapsto \sigma(\alpha) \pmod{\mathfrak{p}}.$$

For this to induce a map in $\mathrm{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right)$, it's necessary that $\sigma(\mathfrak{p}) \subseteq \mathfrak{p}$. So, we consider the subset of automorphisms that fixes $\mathfrak{p}$:

**Definition 61.5.1.** Let $D_\mathfrak{p} \subseteq \mathrm{Gal}(K/\mathbb{Q})$ be the stabilizer of $\mathfrak{p}$, that is

$$D_\mathfrak{p} \coloneqq \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma\mathfrak{p} = \mathfrak{p}\}.$$

We say $D_\mathfrak{p}$ is the **decomposition group** of $\mathfrak{p}$.

Note that this definition is in fact equivalent to the set of $\sigma$ such that $\sigma(\mathfrak{p}) \subseteq \mathfrak{p}$, because a field isomorphism fixes the ideal norm $\mathrm{N}(\mathfrak{p})$.

So there's a natural map

$$D_\mathfrak{p} \xrightarrow{\theta} \mathrm{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right)$$

by declaring $\theta(\sigma)$ to just be "$\sigma \pmod{\mathfrak{p}}$". The fact that $\sigma \in D_\mathfrak{p}$ (i.e. $\sigma$ fixes $\mathfrak{p}$) ensures this map is well-defined.

Surprisingly, every element of $\mathrm{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right)$ arises this way from some field automorphism of $K$.

**Theorem 61.5.2** (Decomposition group and Galois group)

Define $\theta$ as above. Then

- $\theta$ is surjective, and
- its kernel is a group of order $e$, the ramification index.

In particular, if $p$ is unramified then $D_\mathfrak{p} \cong \mathrm{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right)$.

(The proof is not hard, but a bit lengthy and in my opinion not very enlightening.)

**If $p$ is unramified, then taking modulo $\mathfrak{p}$ gives $D_{\mathfrak{p}} \cong \mathrm{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right)$.**

But we know exactly what $\mathrm{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right)$ is! We already have $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f}$, and the Galois group is

$$\mathrm{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right) \cong \mathrm{Gal}\left(\mathbb{F}_{p^f}/\mathbb{F}_p\right) \cong \langle x \mapsto x^p \rangle \cong \mathbb{Z}/f\mathbb{Z}.$$

So

$$D_{\mathfrak{p}} \cong \mathbb{Z}/f\mathbb{Z}$$

as well.

Let's now go back to

$$D_{\mathfrak{p}} \xrightarrow{\theta} \mathrm{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right).$$

The kernel of $\theta$ is called the **inertia group** and denoted $I_{\mathfrak{p}} \subseteq D_{\mathfrak{p}}$; it has order $e$.

This gives us a pretty cool sequence of subgroups $\{1\} \subseteq I \subseteq D \subseteq G$ where $G$ is the Galois group (I'm dropping the $\mathfrak{p}$-subscripts now). Let's look at the corresponding *fixed fields* via the Fundamental theorem of Galois theory. Picture:

$$\begin{array}{lcc}
\mathfrak{p} \subset \mathcal{O}_K \subset & K & \{1\} \\
& \uparrow \text{Ramify} & \downarrow e \\
& K^I & I \\
& \uparrow \text{Inert} & \downarrow f \\
& K^D & D \\
& \uparrow \text{Split} & \downarrow g \\
(p) \subset \mathbb{Z} \subset & \mathbb{Q} & G
\end{array}$$

Something curious happens:

- If $D \trianglelefteq G$, when $(p)$ is lifted into $K^D$ it splits completely into $g$ unramified primes. Each of these has inertial degree 1.
- If $I \trianglelefteq G$ as well, when the primes in $K^D$ are lifted to $K^I$, they remain inert, and now have inertial degree $f$.
- When they're then lifted to $K$, they ramify with exponent $e$ (but don't split at all).

In other words, the process of going from 1 to $efg$ can be very nicely broken into the three steps above. To draw this in the picture, we get

$$(p) \longrightarrow \mathfrak{p}_1' \dots \mathfrak{p}_g' \longrightarrow \mathfrak{p}_1'' \dots \mathfrak{p}_g'' \longrightarrow (\mathfrak{p}_1 \dots \mathfrak{p}_g)^e$$

$$\{f_i\}: \qquad 1, \dots, 1 \qquad f, \dots, f \qquad f, \dots, f$$

$$\mathbb{Q} \overset{\text{Split}}{\text{———}} K^D \overset{\text{Inert}}{\text{———}} K^I \overset{\text{Ramify}}{\text{———}} K$$

In any case, in the "typical" case that there is no ramification, we just have $K^I = K$.

**Example 61.5.3** (Primes split before remaining inert)

Let $K = \mathbb{Q}[\zeta_5]$ where $\zeta_5$ is a primitive 5th root of unity. From Problem 59A$^\star$, we know that the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}$.

Let $p = 19$. In $K$, $p$ factors as $19 = (2\sqrt{5}+1)(2\sqrt{5}-1)$, and luckily for us, $\mathcal{O}_K$ is a principal ideal domain, which means the ideal $(19)$ factors as $(19) = \mathfrak{p}_1\mathfrak{p}_2 = (2\sqrt{5}+1)(2\sqrt{5}-1)$.

In this case, we have $K^{D_{\mathfrak{p}_1}} = K^D = \mathbb{Q}[\sqrt{5}]$ and $K^I = K$, and indeed:

- When $(19)$ is lifted to $K^D$, it already splits into $(2\sqrt{5}+1)(2\sqrt{5}-1)$ — because $2\sqrt{5}+1 \in K^D$. As $[K^D : \mathbb{Q}] = 2$ and $(19)$ already split into 2 primes, each of the prime necessarily have inertial degree 1.
- When each of $(2\sqrt{5}+1)$ and $(2\sqrt{5}-1)$ is lifted from $K^D$ to $K$, they remains inert. Again, as $[K : K^D] = 2$, the inertial degree must be 2.

Part of the theorem can be seen very easily: by the fundamental theorem of Galois theory, because all of the field automorphisms in $D$ fixes $2\sqrt{5}+1$, then tautologically, $2\sqrt{5}+1$ must belong to the fixed field of $D$! In other words, $2\sqrt{5}+1 \in K^D$, which means $p$ already splits when lifted to $K^D$.

The argument only need to be modified a little to show $\mathfrak{p}_1' = \mathfrak{p}_1 \cap K^D$ does not split when lifted from $K^D$ to $K$: because the extension $K/K^D$ is Galois, the Galois group $\mathrm{Gal}(K/K^D)$ acts transitively on the primes $\mathfrak{p}_i$ above $\mathfrak{p}_1' = (2\sqrt{5}+1) \subseteq K^D$, but once again, $\mathfrak{p}_1$ is the only prime in the orbit by the definition of $D$.

**Example 61.5.4** (Different primes have different $K^D$)

When $D \not\trianglelefteq G$, there need not be a single subfield $K^D$ that $p$ splits cleanly into $\mathfrak{p}_1 \dots \mathfrak{p}_g$ when lifted to that field.

The reason is simple — each prime $\mathfrak{p}_i$ gets split from the product in its *own* $K^{D_{\mathfrak{p}_i}}$, but if $D_{\mathfrak{p}_1}$ is not normal in $G$, then the different $D_{\mathfrak{p}_i}$ are not the same — instead, they're conjugate subgroups of $G$.

Let us take a concrete example: let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. The rational prime $p = (5)$ splits as $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ in $K$, and each has inertial degree 2. Thus $|D_{\mathfrak{p}_i}| = 2$ for each $i$.

We know that $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$, and $S_3$ has no subgroups of order 2, so obviously $D_{\mathfrak{p}_i}$ is not normal in $G$!

As mentioned above, what happens here is: when $p$ is lifted to $K^{D_{\mathfrak{p}_1}}$, it splits into $\mathfrak{p}_1'\mathfrak{p}_{23}'$, with $\mathfrak{p}_1$ above $\mathfrak{p}_1'$ and both $\mathfrak{p}_2$ and $\mathfrak{p}_3$ above $\mathfrak{p}_{23}'$. In the extension $K^{D_{\mathfrak{p}_1}}/\mathbb{Q}$, $\mathfrak{p}_1'$ has inertial degree 1 as before, but $\mathfrak{p}_{23}'$ has inertial degree 2.

## §61.6 Tangential remark: more general Galois extensions

All the discussion about Galois extensions carries over if we replace $K/\mathbb{Q}$ by some different Galois extension $K/F$. Instead of a rational prime $p$ breaking down in $\mathcal{O}_K$, we would have a prime ideal $\mathfrak{p}$ of $F$ breaking down as

$$\mathfrak{p} \cdot \mathcal{O}_L = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e$$

in $\mathcal{O}_L$ and then all results hold verbatim. (The $\mathfrak{P}_i$ are primes in $L$ above $\mathfrak{p}$.) Instead of $\mathbb{F}_p$ we would have $\mathcal{O}_F/\mathfrak{p}$.

The reason I choose to work with $F = \mathbb{Q}$ is that capital Gothic $P$'s ($\mathfrak{P}$) look *really* terrifying.

## §61.7 A few harder problems to think about

more problems

**Problem 61A$^\dagger$.** Prove that no rational prime $p$ can remain inert in $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$, the splitting field of $x^3 - 2$. How does this generalize?

# 62 The Frobenius element

Throughout this chapter $K/\mathbb{Q}$ is a Galois extension with Galois group $G$, $p$ is an *unramified* rational prime in $K$, and $\mathfrak{p}$ is a prime above it. Picture:

$$\begin{array}{ccccc} K & \supset & \mathcal{O}_K & \mathfrak{p} & \mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f} \\ | & & | & | & | \\ \mathbb{Q} & \supset & \mathbb{Z} & (p) & \mathbb{F}_p \end{array}$$

We recall that the $p$-th power map $\sigma\colon \mathbb{F}_{p^f} \to \mathbb{F}_{p^f}$ is an automorphism, and it's called the Frobenius map on $\mathbb{F}_{p^f}$. We can try to extend this map to a $K \to K$ map by $\sigma(x) = x^p$, unfortunately this doesn't make it a field automorphism.

Surprisingly, it is nevertheless possible to extend this to some field automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

If $p$ is unramified, then one can show there is a unique $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\alpha) \equiv \alpha^p \pmod{\mathfrak{p}}$ for every prime $p$.

## §62.1 Frobenius elements

*Prototypical example for this section:* $\mathrm{Frob}_{\mathfrak{p}}$ *in* $\mathbb{Z}[i]$ *depends on* $p \pmod 4$.

Here is the theorem statement again:

**Theorem 62.1.1** (The Frobenius element)

Assume $K/\mathbb{Q}$ is Galois with Galois group $G$. Let $p$ be a rational prime unramified in $K$, and $\mathfrak{p}$ a prime above it. There is a *unique* element $\mathrm{Frob}_{\mathfrak{p}} \in G$ with the property that, for all $\alpha \in \mathcal{O}_K$,

$$\mathrm{Frob}_{\mathfrak{p}}(\alpha) \equiv \alpha^p \pmod{\mathfrak{p}}.$$

It is called the **Frobenius element** at $\mathfrak{p}$, and has order $f$.

The *uniqueness* part is pretty important: it allows us to show that a given $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is the Frobenius element by just observing that it satisfies the above functional equation.

Let's see an example of this:

**Example 62.1.2** (Frobenius elements of the Gaussian integers)

Let's actually compute some Frobenius elements for $K = \mathbb{Q}(i)$, which has $\mathcal{O}_K = \mathbb{Z}[i]$. This is a Galois extension, with $G = (\mathbb{Z}/2\mathbb{Z})^\times$, corresponding to the identity and complex conjugation.

If $p$ is an odd prime with $\mathfrak{p}$ above it, then $\mathrm{Frob}_{\mathfrak{p}}$ is the unique element such that

$$(a+bi)^p \equiv \mathrm{Frob}_{\mathfrak{p}}(a+bi) \pmod{\mathfrak{p}}$$

in $\mathbb{Z}[i]$. In particular,

$$\text{Frob}_{\mathfrak{p}}(i) = i^p = \begin{cases} i & p \equiv 1 \pmod 4 \\ -i & p \equiv 3 \pmod 4. \end{cases}$$

From this we see that $\text{Frob}_{\mathfrak{p}}$ is the identity when $p \equiv 1 \pmod 4$ and $\text{Frob}_{\mathfrak{p}}$ is complex conjugation when $p \equiv 3 \pmod 4$.

Note that we really only needed to compute $\text{Frob}_{\mathfrak{p}}$ on $i$. If this seems too good to be true, a philosophical reason is "freshman's dream" where $(x+y)^p \equiv x^p + y^p \pmod p$ (and hence mod $\mathfrak{p}$). So if $\sigma$ satisfies the functional equation on generators, it satisfies the functional equation everywhere.

We also have an important lemma:

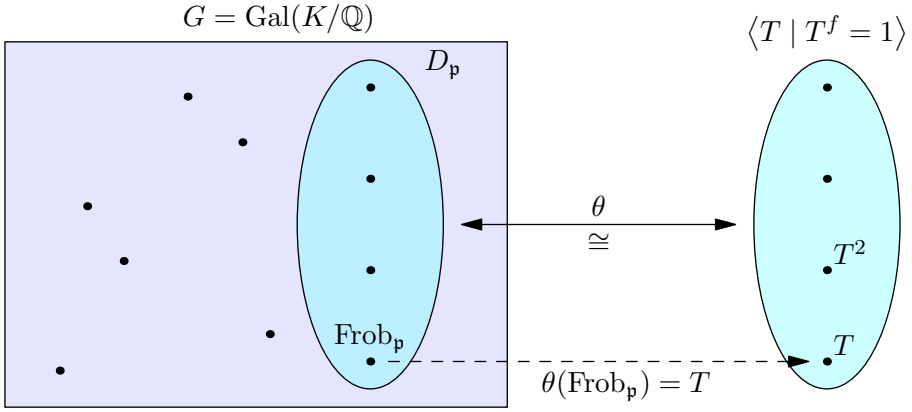
**Lemma 62.1.3** (Order of the Frobenius element)
Let $\text{Frob}_{\mathfrak{p}}$ be a Frobenius element from an extension $K/\mathbb{Q}$. Then the order of $\text{Frob}_{\mathfrak{p}}$ is equal to the inertial degree $f_{\mathfrak{p}}$. In particular, $(p)$ splits completely in $\mathcal{O}_K$ if and only if $\text{Frob}_{\mathfrak{p}} = \text{id}$.

This lemma allows us to tell the splitting behavior of $\mathfrak{p}$ just by computing $\text{Frob}_{\mathfrak{p}}$, which will later be seen in Lemma 62.4.1 and Section 62.6.iii.

**Exercise 62.1.4.** Prove this lemma as by using the fact that $\mathcal{O}_K/\mathfrak{p}$ is the finite field of order $f_{\mathfrak{p}}$, and the Frobenius element is just $x \mapsto x^p$ on this field.

Let us now prove the main theorem. This will only make sense in the context of decomposition groups, so readers which skipped that part should omit this proof.

*Proof of existence of Frobenius element.* The entire theorem is just a rephrasing of the fact that the map $\theta$ defined in the last section is an isomorphism when $p$ is unramified. Picture:




In here we can restrict our attention to $D_{\mathfrak{p}}$ since we need to have $\sigma(\alpha) \equiv 0 \pmod{\mathfrak{p}}$ when $\alpha \equiv 0 \pmod{\mathfrak{p}}$. Thus we have the isomorphism

$$D_{\mathfrak{p}} \xrightarrow{\theta} \text{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right).$$

But we already know $\text{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right)$, according to the string of isomorphisms

$$\text{Gal}\left((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p\right) \cong \text{Gal}\left(\mathbb{F}_{p^f}/\mathbb{F}_p\right) \cong \langle T = x \mapsto x^p \rangle \cong \mathbb{Z}/f\mathbb{Z}.$$

So the unique such element is the pre-image of $T$ under $\theta$. □

## §62.2 Conjugacy classes

Now suppose $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are *two* primes above an unramified rational prime $p$. Then we can define $\text{Frob}_{\mathfrak{p}_1}$ and $\text{Frob}_{\mathfrak{p}_2}$. Since the Galois group acts transitively, we can select $\sigma \in \text{Gal}(K/\mathbb{Q})$ be such that

$$\sigma(\mathfrak{p}_1) = \mathfrak{p}_2.$$

We claim that

$$\text{Frob}_{\mathfrak{p}_2} = \sigma \circ \text{Frob}_{\mathfrak{p}_1} \circ \sigma^{-1}.$$

Note that this is an equation in $G$.

**Question 62.2.1.** Prove this.

More generally, for a given unramified rational prime $p$, we obtain:

**Theorem 62.2.2** (Conjugacy classes in Galois groups)
The set

$$\{\text{Frob}_{\mathfrak{p}} \mid \mathfrak{p} \text{ above } p\}$$

is one of the conjugacy classes of $G$.

*Proof.* We've used the fact that $G = \text{Gal}(K/\mathbb{Q})$ is transitive to show that $\text{Frob}_{\mathfrak{p}_1}$ and $\text{Frob}_{\mathfrak{p}_2}$ are conjugate if they both lie above $p$; hence it's *contained* in some conjugacy class. So it remains to check that for any $\mathfrak{p}$, $\sigma$, we have $\sigma \circ \text{Frob}_{\mathfrak{p}} \circ \sigma^{-1} = \text{Frob}_{\mathfrak{p}'}$ for some $\mathfrak{p}'$. For this, just take $\mathfrak{p}' = \sigma\mathfrak{p}$. Hence the set is indeed a conjugacy class. □

In summary,

**$\text{Frob}_{\mathfrak{p}}$ is determined up to conjugation by the prime $p$ from which $\mathfrak{p}$ arises.**

So even though the Gothic letters look scary, the content of $\text{Frob}_{\mathfrak{p}}$ really just comes from the more friendly-looking rational prime $p$.

**Example 62.2.3** (Frobenius elements in $\mathbb{Q}(\sqrt[3]{2}, \omega)$)
With those remarks, here is a more involved example of a Frobenius map. Let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ be the splitting field of

$$t^3 - 2 = (t - \sqrt[3]{2})(t - \omega\sqrt[3]{2})(t - \omega^2\sqrt[3]{2}).$$

Thus $K/\mathbb{Q}$ is Galois. We've seen in an earlier example that

$$\mathcal{O}_K = \mathbb{Z}[\varepsilon] \quad \text{where} \quad \varepsilon \text{ is a root of } t^6 + 3t^5 - 5t^3 + 3t + 1.$$

Let's consider the prime 5 which factors (trust me here) as

$$(5) = (5, \varepsilon^2 + \varepsilon + 2)(5, \varepsilon^2 + 3\varepsilon + 3)(5, \varepsilon^2 + 4\varepsilon + 1) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3.$$

Note that all the prime ideals have inertial degree 2. Thus $\text{Frob}_{\mathfrak{p}_i}$ will have order 2 for each $i$.

Note that

$$\text{Gal}(K/\mathbb{Q}) = \text{permutations of } \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\} \cong S_3.$$

In this $S_3$ there are 3 elements of order two: fixing one root and swapping the other two. These correspond to each of $\text{Frob}_{\mathfrak{p}_1}$, $\text{Frob}\mathfrak{p}_2$, $\text{Frob}_{\mathfrak{p}_3}$.

In conclusion, the conjugacy class $\{\text{Frob}_{\mathfrak{p}_1}, \text{Frob}_{\mathfrak{p}_2}, \text{Frob}_{\mathfrak{p}_3}\}$ associated to (5) is the cycle type $(\bullet)(\bullet\,\bullet)$ in $S_3$.

## §62.3 Chebotarev density theorem

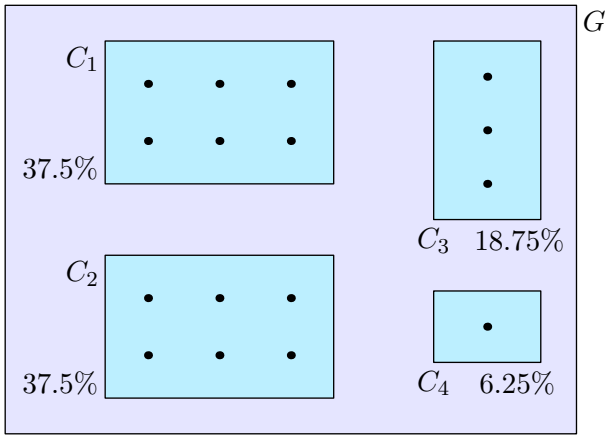
Natural question: can we represent every conjugacy class in this way? In other words, is every element of $G$ equal to $\text{Frob}_{\mathfrak{p}}$ for some $\mathfrak{p}$?

Miraculously, not only is the answer "yes", but in fact it does so in the nicest way possible: the $\text{Frob}_{\mathfrak{p}}$'s are "equally distributed" when we pick a random $\mathfrak{p}$.

**Theorem 62.3.1** (Chebotarev density theorem over $\mathbb{Q}$)
Let $C$ be a conjugacy class of $G = \text{Gal}(K/\mathbb{Q})$. The density of (unramified) primes $p$ such that $\{\text{Frob}_{\mathfrak{p}} \mid \mathfrak{p} \text{ above } p\} = C$ is exactly $|C| / |G|$. In particular, for any $\sigma \in G$ there are infinitely many rational primes $p$ with $\mathfrak{p}$ above $p$ so that $\text{Frob}_{\mathfrak{p}} = \sigma$.

By density, I mean that the proportion of primes $p \le x$ that work approaches $\frac{|C|}{|G|}$ as $x \to \infty$. Note that I'm throwing out the primes that ramify in $K$. This is no issue, since the only primes that ramify are those dividing $\Delta_K$, of which there are only finitely many.

In other words, if I pick a random prime $p$ and look at the resulting conjugacy class, it's a lot like throwing a dart at $G$: the probability of hitting any conjugacy class depends just on the size of the class.




**Remark 62.3.2** — Happily, this theorem (and preceding discussion) also works if we replace $K/\mathbb{Q}$ with any Galois extension $K/F$; in that case we replace "$\mathfrak{p}$ over $p$" with "$\mathfrak{P}$ over $\mathfrak{p}$". In that case, we use $\text{N}(\mathfrak{p}) \le x$ rather than $p \le x$ as the way to define density.

## §62.4 Example: Frobenius elements of cyclotomic fields

Let $q$ be a prime, and consider $L = \mathbb{Q}(\zeta_q)$, with $\zeta_q$ a primitive $q$th root of unity. You should recall from various starred problems that

- $\Delta_L = \pm q^{q-2}$,

- $\mathcal{O}_L = \mathbb{Z}[\zeta_q]$, and
- The map
$$\sigma_n \colon L \to L \quad \text{by} \quad \zeta_q \mapsto \zeta_q^n$$
is an automorphism of $L$ whenever $\gcd(n,q) = 1$, and depends only on $n \pmod q$. In other words, the automorphisms of $L/\mathbb{Q}$ just shuffle around the $q$th roots of unity. In fact the Galois group consists exactly of the elements $\{\sigma_n\}$, namely
$$\mathrm{Gal}(L/\mathbb{Q}) = \{\sigma_n \mid n \not\equiv 0 \pmod q\}.$$
As a group,
$$\mathrm{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}.$$

This is surprisingly nice, because **elements of** $\mathrm{Gal}(L/\mathbb{Q})$ **look a lot like Frobenius elements already**. Specifically:

**Lemma 62.4.1** (Cyclotomic Frobenius elements)
In the cyclotomic setting $L = \mathbb{Q}(\zeta_q)$, let $p$ be a rational unramified prime and $\mathfrak{p}$ above it. Then
$$\mathrm{Frob}_{\mathfrak{p}} = \sigma_p.$$

*Proof.* Observe that $\sigma_p$ satisfies the functional equation (check on generators). Done by uniqueness. □

**Question 62.4.2.** Conclude that a rational prime $p$ splits completely in $\mathcal{O}_L$ if and only if $p \equiv 1 \pmod q$.

## §62.5 Frobenius elements behave well with restriction

Let $L/\mathbb{Q}$ and $K/\mathbb{Q}$ be Galois extensions, and consider the setup

$$\begin{array}{ccccc}
L & \supset & \mathfrak{P} & \dashrightarrow & \mathrm{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(L/\mathbb{Q}) \\
| & & | & & \\
K & \supset & \mathfrak{p} & \dashrightarrow & \mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q}) \\
| & & | & & \\
\mathbb{Q} & \supset & (p) & &
\end{array}$$

Here $\mathfrak{p}$ is above $(p)$ and $\mathfrak{P}$ is above $\mathfrak{p}$. We may define
$$\mathrm{Frob}_{\mathfrak{p}} \colon K \to K \quad \text{and} \quad \mathrm{Frob}_{\mathfrak{P}} \colon L \to L$$
and want to know how these are related.

Both maps $\mathrm{Frob}_{\mathfrak{P}}$ and $\mathrm{Frob}_{\mathfrak{p}}$ induce the power-of-$p$ map in the corresponding quotient field, hence we would expect them to be naturally the same.

**Theorem 62.5.1** (Restrictions of Frobenius elements)
Assume $L/\mathbb{Q}$ and $K/\mathbb{Q}$ are both Galois. Let $\mathfrak{P}$ and $\mathfrak{p}$ be unramified as above. Then $\text{Frob}_{\mathfrak{P}}|_K = \text{Frob}_{\mathfrak{p}}$, i.e. for every $\alpha \in K$,

$$\text{Frob}_{\mathfrak{p}}(\alpha) = \text{Frob}_{\mathfrak{P}}(\alpha).$$

*Proof.* First, $K/\mathbb{Q}$ is normal, so $\text{Frob}_{\mathfrak{P}}$ fixes the image of $K$, that is, $\text{Frob}_{\mathfrak{P}}|_K \in \text{Gal}(K/\mathbb{Q})$ is well-defined.

We have the natural map $\phi\colon \mathcal{O}_K \to \mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P}$, and the quotient map $q\colon \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$. Since $\mathfrak{p} \subseteq \mathfrak{P} \cap \mathcal{O}_K \subseteq \ker \phi$, it follows $\phi$ factors through $q$ to give a natural field homomorphism $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_L/\mathfrak{P}$.

Since a field homomorphism is injective, $\text{Frob}_{\mathfrak{P}}$ induces the power-of-$p$ map on $\mathcal{O}_L/\mathfrak{P}$, and everything is commutative, the theorem follows. □

In short, the point of this section is that

**Frobenius elements upstairs restrict to Frobenius elements downstairs.**

## §62.6 Application: Quadratic reciprocity

We now aim to prove:

**Theorem 62.6.1** (Quadratic reciprocity)
Let $p$ and $q$ be distinct odd primes. Then

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

(See, e.g. [Le] for an exposition on quadratic reciprocity, if you're not familiar with it.)

### §62.6.i Step 1: Setup

For this proof, we first define

$$L = \mathbb{Q}(\zeta_q)$$

where $\zeta_q$ is a primitive $q$th root of unity. Then $L/\mathbb{Q}$ is Galois, with Galois group $G$.

**Question 62.6.2.** Show that $G$ has a unique subgroup $H$ of index two.

In fact, we can describe it exactly: viewing $G \cong (\mathbb{Z}/q\mathbb{Z})^\times$, we have

$$H = \{\sigma_n \mid n \text{ quadratic residue mod } q\}.$$

By the fundamental theorem of Galois Theory, there ought to be a degree 2 extension of $\mathbb{Q}$ inside $\mathbb{Q}(\zeta_q)$ (that is, a quadratic field). Call it $\mathbb{Q}(\sqrt{q^*})$, for $q^*$ squarefree:

$$\begin{array}{ccc} L = \mathbb{Q}(\zeta_q) & \longleftrightarrow & \{1\} \\ {\scriptstyle \frac{q-1}{2}}\big| & & \big| \\ K = \mathbb{Q}(\sqrt{q^*}) & \longleftrightarrow & H \\ {\scriptstyle 2}\big| & & \big| \\ \mathbb{Q} & \longleftrightarrow & G \end{array}$$

**Exercise 62.6.3.** Note that if a rational prime $\ell$ ramifies in $K$, then it ramifies in $L$. Use this to show that

$$q^* = \pm q \text{ and } q^* \equiv 1 \pmod 4.$$

Together these determine the value of $q^*$.

(Actually, it is true in general $\Delta_K$ divides $\Delta_L$ in a tower $L/K/\mathbb{Q}$.)

## §62.6.ii Step 2: Reformulation

Now we are going to prove:

**Theorem 62.6.4** (Quadratic reciprocity, equivalent formulation)
For distinct odd primes $p$, $q$ we have

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right).$$

**Exercise 62.6.5.** Using the fact that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, show that this is equivalent to quadratic reciprocity as we know it.

We look at the rational prime $p$ in $\mathbb{Z}$. Either it splits into two in $K$ or is inert; either way let $\mathfrak{p}$ be a prime factor in the resulting decomposition (so $\mathfrak{p}$ is either $p \cdot \mathcal{O}_K$ in the inert case, or one of the primes in the split case). Then let $\mathfrak{P}$ be above $\mathfrak{p}$. It could possibly also split in $K$: the picture looks like

$$\begin{array}{ccccc}
\mathcal{O}_L = \mathbb{Z}[\zeta_q] & \supset & \mathfrak{P} & \dashrightarrow & \mathbb{Z}[\zeta_q]/\mathfrak{P} \cong \mathbb{F}_{p^f} \\
\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{q^*}}{2}] & \supset & \mathfrak{p} & \dashrightarrow & \mathbb{F}_p \text{ or } \mathbb{F}_{p^2} \\
\mathbb{Z} & \supset & (p) & \dashrightarrow & \mathbb{F}_p
\end{array}$$

**Question 62.6.6.** Why is $p$ not ramified in either $K$ or $L$?

## §62.6.iii Step 3: Introducing the Frobenius

Now, we take the Frobenius

$$\sigma_p = \text{Frob}_{\mathfrak{P}} \in \text{Gal}(L/\mathbb{Q}).$$

We claim that

$$\text{Frob}_{\mathfrak{P}} \in H \iff p \text{ splits in } K.$$

To see this, note that $\text{Frob}_{\mathfrak{P}}$ is in $H$ if and only if it acts as the identity on $K$. But $\text{Frob}_{\mathfrak{P}}\restriction_K$ is $\text{Frob}_{\mathfrak{p}}$! So

$$\text{Frob}_{\mathfrak{P}} \in H \iff \text{Frob}_{\mathfrak{p}} = \text{id}_K.$$

Finally, by Lemma 62.1.3, $\text{Frob}_{\mathfrak{p}}$ has order 1 if $p$ splits ($\mathfrak{p}$ has inertial degree 1) and order 2 if $p$ is inert. This completes the proof of the claim.

### §62.6.iv Finishing up

We already know by Lemma 62.4.1 that $\text{Frob}_{\mathfrak{P}} = \sigma_p \in H$ if and only if $p$ is a quadratic residue. On the other hand,

> **Exercise 62.6.7.** Show that $p$ splits in $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(1+\sqrt{q^*})]$ if and only if $\left(\frac{q^*}{p}\right) = 1$. (Use the factoring algorithm. You need the fact that $p \neq 2$ here.)

In other words,

$$\begin{aligned}
\left(\frac{p}{q}\right) = 1 &\iff \sigma_p \in H \\
&\iff \text{Frob}_{\mathfrak{P}} \in H \\
&\iff \text{Frob}_{\mathfrak{p}} = \text{id}_K \\
&\iff \text{ord}\,\text{Frob}_{\mathfrak{p}} = 1 \\
&\iff f_{\mathfrak{p}} = 1 \\
&\iff p \text{ splits in } \mathbb{Z}\left[\tfrac{1}{2}(1+\sqrt{q^*})\right] \\
&\iff \left(\frac{q^*}{p}\right) = 1.
\end{aligned}$$

This completes the proof.

## §62.7 Frobenius elements control factorization

*Prototypical example for this section:* $\text{Frob}_{\mathfrak{p}}$ *controlled the splitting of* $p$ *in the proof of quadratic reciprocity; the same holds in general.*

In the proof of quadratic reciprocity, we used the fact that Frobenius elements behaved well with restriction in order to relate the splitting of $p$ with properties of $\text{Frob}_{\mathfrak{p}}$.

In fact, there is a much stronger statement for any intermediate field $\mathbb{Q} \subseteq E \subseteq K$ which works even if $E/\mathbb{Q}$ is not Galois. It relies on the notion of a *factorization pattern*. Here is how it goes.

Set $n = [E : \mathbb{Q}]$, and let $p$ be a rational prime unramified in $K$. Then $p$ can be broken in $E$ as

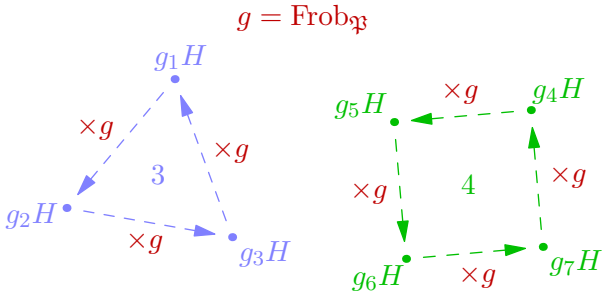
$$p \cdot \mathcal{O}_E = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_g$$

with inertial degrees $f_1, \dots, f_g$: (these inertial degrees might be different since $E/\mathbb{Q}$ isn't Galois). The numbers $f_1 + \dots + f_g = n$ form a partition of the number $n$. For example, in the quadratic reciprocity proof we had $n = 2$, with possible partitions $1+1$ (if $p$ split) and $2$ (if $p$ was inert). We call this the **factorization pattern** of $p$ in $E$.

Next, we introduce a Frobenius $\text{Frob}_{\mathfrak{P}}$ above $(p)$, all the way in $K$; this is an element of $G = \text{Gal}(K/\mathbb{Q})$. Then let $H$ be the group corresponding to the field $E$. Diagram:

$$\begin{array}{ccc}
K & \hookrightarrow & \{1\} \\
| & & | \\
E & \hookrightarrow & H \\
{\scriptstyle n}\,| & & |\,{\scriptstyle n} \\
\mathbb{Q} & \hookrightarrow & G
\end{array}
\qquad
\begin{array}{c}
\text{Frob}_{\mathfrak{P}} \\
\\
\mathfrak{p}_1 \dots \mathfrak{p}_g \\
| \\
(p)
\end{array}
\qquad
f_1 + \dots + f_g = n$$

Then $\text{Frob}_{\mathfrak{P}}$ induces a *permutation* of the $n$ left cosets $gH$ by left multiplication (after all, $\text{Frob}_{\mathfrak{P}}$ is an element of $G$ too!). Just as with any permutation, we may look at the resulting cycle decomposition, which has a natural "cycle structure": a partition of $n$.




$$\boxed{n = 7 = 3 + 4}$$

The theorem is that these coincide:

**Theorem 62.7.1** (Frobenius elements control decomposition)

Let $\mathbb{Q} \subseteq E \subseteq K$ an extension of number fields and assume $K/\mathbb{Q}$ is Galois (though $E/\mathbb{Q}$ need not be). Pick an unramified rational prime $p$; let $G = \text{Gal}(K/\mathbb{Q})$ and $H$ the corresponding intermediate subgroup. Finally, let $\mathfrak{P}$ be a prime above $p$ in $K$.

Then the *factorization pattern* of $p$ in $E$ is given by the *cycle structure* of $\text{Frob}_{\mathfrak{P}}$ acting on the left cosets of $H$.

Often, we take $E = K$, in which case this is just asserting that the decomposition of the prime $p$ is controlled by a Frobenius element over it.

*Sketch of Proof.* Let $\alpha$ be an algebraic integer and $f$ its minimal polynomial (of degree $n$). Set $E = \mathbb{Q}(\alpha)$ (which has degree $n$ over $\mathbb{Q}$). Suppose we're lucky enough that $\mathcal{O}_E = \mathbb{Z}[\alpha]$, i.e. that $E$ is monogenic. Then we know by the Factoring Algorithm, to factor any $p$ in $E$, all we have to do is factor $f$ modulo $p$, since if $f = f_1^{e_1} \dots f_g^{e_g} \pmod p$ then we have

$$(p) = \prod_i \mathfrak{p}_i = \prod_i (f_i(\alpha), p)^{e_i}.$$

This gives us complete information about the ramification indices and inertial degrees; the $e_i$ are the ramification indices, and $\deg f_i$ are the inertial degrees (since $\mathcal{O}_E/\mathfrak{p}_i \cong \mathbb{F}_p[X]/(f_i(X))$).

In particular, if $p$ is unramified then all the $e_i$ are equal to 1, and we get

$$n = \deg f = \deg f_1 + \deg f_2 + \cdots + \deg f_g.$$

Once again we have a partition of $n$; we call this the **factorization pattern** of $f$ modulo $p$. So, to see the factorization pattern of an unramified $p$ in $\mathcal{O}_E$, we just have to know the factorization pattern of $f \pmod p$.

To prove our theorem, we will show that the factorization pattern of $f \pmod p$ corresponds exactly to the cycle decomposition of the action of $\text{Frob}_{\mathfrak{P}}$ on the roots of $f$ and that the roots of $f$ correspond exactly to the cosets of $H$ in $G$.

To do this, suppose $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ are the roots of $f$ (distinct roots since $f$ is irreducible over $\mathbb{Q}$). We let $\text{Frob}_{\mathfrak{P}}$ act on $S$. This splits $S$ into orbits $S_1$, $S_2$, …, $S_k$.

Construct polynomials $f_i$ with coefficients in $E$ having roots exactly the elements of $S_i$. This forms a factorization of $f$ over $E$, say

$$f = f_1 f_2 \dots f_k.$$

We claim that this in fact induces a factorization of $f \pmod p$. To see this, consider the images of these polynomials $f_i$ under the quotient $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{P}$, denote them by $\overline{f_i}$. Then since $p$ is unramified, we know that the decomposition group $D(\mathfrak{P}|p)$ is isomorphic to the Galois group $\mathcal{G} = \mathrm{Gal}((\mathcal{O}_E/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z}))$. Thus $\mathrm{Frob}_\mathfrak{P}$ corresponds to the generator $\sigma$ of $\mathcal{G}$. It is not hard to believe that the action of $\mathrm{Frob}_\mathfrak{P}$ on the roots of $f$ is the same as that of $\sigma$ on the roots of $\overline{f}$. Since the roots of $f_i$ form an orbit under the action of $\mathrm{Frob}_\mathfrak{P}$, we see that the roots of $\overline{f_i}$ form an orbit under the action of $\sigma$ and hence under the action of $\mathcal{G}$. It is now a standard fact of Galois theory that $\overline{f_i}$ is an irreducible polynomial over $\mathbb{F}_p$ (since it is fixed by $\mathcal{G}$), thus the claim is proved.

Now we just need to observe that the roots of $f$ correspond to the cosets of $H$, this will be established later. □

We saw above that given the factorization pattern of $f \pmod p$, we can determine the factorization pattern of an unramified prime $p$ in $\mathcal{O}_E$.

Turning this on its head, if we want to know the factorization pattern of $f \pmod p$, we just need to know how $p$ decomposes. And it turns out these coincide even without the assumption that $E$ is monogenic.

**Theorem 62.7.2** (Frobenius controls polynomial factorization)

Let $\alpha$ be an algebraic integer with minimal polynomial $f$, and let $E = \mathbb{Q}(\alpha)$. Then for any prime $p$ unramified in the splitting field $K$ of $f$, the following coincide:

(i) The factorization pattern of $p$ in $E$.

(ii) The factorization pattern of $f \pmod p$.

(iii) The cycle structure associated to the action of $\mathrm{Frob}_\mathfrak{P} \in \mathrm{Gal}(K/\mathbb{Q})$ on the roots of $f$, where $\mathfrak{P}$ is above $p$ in $K$.

**Example 62.7.3** (Factoring $x^3 - 2 \pmod 5$)

Let $\alpha = \sqrt[3]{2}$ and $f = x^3 - 2$, so $E = \mathbb{Q}(\sqrt[3]{2})$. Set $p = 5$ and finally, let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ be the splitting field. Setup:

$$\begin{array}{ccc}
K = \mathbb{Q}(\sqrt[3]{2}, \omega) & \mathfrak{P} & x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2) \\
\Big| 2 & \Big| & \\
E = \mathbb{Q}(\sqrt[3]{2}) & \mathfrak{p} & x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}) \\
\Big| 3 & \Big| & \\
\mathbb{Q} & (5) & x^3 - 2 \text{ irreducible over } \mathbb{Q}
\end{array}$$

The three claimed objects now all have shape $2 + 1$:

(i) By the Factoring Algorithm, we have $(5) = (5, \sqrt[3]{2} - 3)(5, 9 + 3\sqrt[3]{2} + \sqrt[3]{4})$.

(ii) We have $x^3 - 2 \equiv (x - 3)(x^2 + 3x + 9) \pmod 5$.

(iii) We saw before that $\text{Frob}_{\mathfrak{P}} = (\bullet)(\bullet\ \bullet)$.

*Sketch of Proof.* Letting $n = \deg f$. Let $H$ be the subgroup of $G = \text{Gal}(K/\mathbb{Q})$ corresponding to $E$, so $|G/H| = n$. Pictorially, we have

$$\begin{array}{ccc} K & \{1\} & \mathfrak{P} \\ | & | & | \\ E = \mathbb{Q}(\alpha) & H & \mathfrak{p} \\ | & | & | \\ \mathbb{Q} & G & (p) \end{array}$$

We claim that (i), (ii), (iii) are all equivalent to

(iv) The pattern of the action of $\text{Frob}_{\mathfrak{P}}$ on the $G/H$.

In other words we claim the cosets correspond to the $n$ roots of $f$ in $K$. Indeed $H$ is just the set of $\tau \in G$ such that $\tau(\alpha) = \alpha$, so there's a bijection between the roots and the cosets $G/H$ by $\tau H \mapsto \tau(\alpha)$. Think of it this way: if $G = S_n$, and $H = \{\tau : \tau(1) = 1\}$, then $G/H$ has order $n!/(n-1)! = n$ and corresponds to the elements $\{1, \dots, n\}$. So there is a natural bijection from (iii) to (iv).

The fact that (i) is in bijection to (iv) was the previous theorem, Theorem 62.7.1. The correspondence (i) $\iff$ (ii) is a fact of Galois theory, so we omit the proof here. □

All this can be done in general with $\mathbb{Q}$ replaced by $F$; for example, in [Le02].

## §62.8 Example application: IMO 2003 problem 6

As an example of the power we now have at our disposal, let's prove:


**Problem 6.** Let $p$ be a prime number. Prove that there exists a prime number $q$ such that for every integer $n$, the number $n^p - p$ is not divisible by $q$.

We will show, much more strongly, that there exist infinitely many primes $q$ such that $X^p - p$ is irreducible modulo $q$.

*Solution.* Okay! First, we draw the tower of fields

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[p]{p}) \subseteq K$$

where $K$ is the splitting field of $f(x) = x^p - p$. Let $E = \mathbb{Q}(\sqrt[p]{p})$ for brevity and note it has degree $[E : \mathbb{Q}] = p$. Let $G = \text{Gal}(K/\mathbb{Q})$.

**Question 62.8.1.** Show that $p$ divides the order of $G$. (Look at $E$.)

Hence by Cauchy's theorem (Problem 17A$^\star$, which is a purely group-theoretic fact) we can find a $\sigma \in G$ of order $p$. By Chebotarev, there exist infinitely many rational (unramified) primes $q \neq p$ and primes $\mathfrak{Q} \subseteq \mathcal{O}_K$ above $q$ such that $\text{Frob}_{\mathfrak{Q}} = \sigma$. (Yes, that's an uppercase Gothic $Q$. Sorry.)

We claim that all these $q$ work.

By Theorem 62.7.2, the factorization of $f \pmod q$ is controlled by the action of $\sigma = \text{Frob}_{\mathfrak{Q}}$ on the roots of $f$. But $\sigma$ has prime order $p$ in $G$! So all the lengths in the cycle structure have to divide $p$. Thus the possible factorization patterns of $f$ are

$$p = \underbrace{1+1+\cdots+1}_{p \text{ times}} \quad \text{or} \quad p = p.$$

So we just need to rule out the $p = 1 + \cdots + 1$ case now: this only happens if $f$ breaks into linear factors mod $q$. Intuitively this edge case seems highly unlikely (are we really so unlucky that $f$ factors into *linear* factors when we want it to be irreducible?). And indeed this is easy to see: this means that $\sigma$ fixes all of the roots of $f$ in $K$, but that means $\sigma$ fixes $K$ altogether, and hence is the identity of $G$, contradiction. □

**Remark 62.8.2 —** In fact $K = \mathbb{Q}(\sqrt[p]{p}, \zeta_p)$, and $|G| = p(p-1)$. With a little more group theory, we can show that in fact the density of primes $q$ that work is $\frac{1}{p}$.

## §62.9 A few harder problems to think about

**Problem 62A.** Show that for an odd prime $p$,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}.$$

**Problem 62B.** Let $f$ be a nonconstant polynomial with integer coefficients. Suppose $f \pmod p$ splits completely into linear factors for all sufficiently large primes $p$. Show that $f$ splits completely into linear factors.

**Problem 62C$^\dagger$** (Dirichlet's theorem on arithmetic progressions)**.** Let $a$ and $m$ be relatively prime positive integers. Show that the density of primes $p \equiv a \pmod m$ is exactly $\frac{1}{\phi(m)}$.

**Problem 62D.** Let $n$ be an odd integer which is not a prime power. Show that the $n$th cyclotomic polynomial is not irreducible modulo *any* rational prime.

**Problem 62E** (Putnam 2012 B6)**.** Let $p$ be an odd prime such that $p \equiv 2 \pmod 3$. Let $\pi$ be a permutation of $\mathbb{F}_p$ by $\pi(x) = x^3 \pmod p$. Show that $\pi$ is even if and only if $p \equiv 3 \pmod 4$.

# 63 Bonus: A Bit on Artin Reciprocity

In this chapter, I'm going to state some big theorems of global class field theory and use them to deduce the Kronecker-Weber plus Hilbert class fields. No proofs, but hopefully still appreciable. For experts: this is global class field theory, without ideles.

Here's the executive summary: let $K$ be a number field. Then all abelian extensions $L/K$ can be understood using solely information intrinsic to $K$: namely, the ray class groups (generalizing ideal class groups).

## §63.1 Overview

At the end of this section, for an Abelian field extension $L/K$, we will define the Artin symbol

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

which generalizes the Legendre symbol $\left(\frac{a}{p}\right)$:

- Above the solidus, instead of an integer $a$, we have a field extension $L/K$.
- Below the solidus, instead of a rational prime $p$, we have a prime ideal $\mathfrak{p}$ of $K$.

We require $\mathfrak{p}$ to not ramify in the extension $L/K$ for the symbol to be defined.

And, at the end, we want to state the Artin reciprocity theorem, which looks something like the following:

**For primes $\mathfrak{p}$, $\left(\frac{L/K}{\mathfrak{p}}\right)$ depends only on "$\mathfrak{p} \pmod{\mathfrak{f}}$".**

Here, $\mathfrak{f}$ is a "modulus", which only depends on the field extension $L/K$.

In order to do that, we first need to define what it means for two ideals to be coprime modulo something. We will divide up the ideals of $\mathcal{O}_K$ that is "coprime" to $\mathfrak{f}$ into "residue classes modulo $\mathfrak{f}$" (we will call them "ray classes" from now on) in such a way that:

- It generalizes the class group – two ideals that belong to different ideal classes (i.e. are nonisomorphic as $\mathcal{O}_K$-modules) belong to different ray classes.
- It respects the multiplicative structure – if $\mathfrak{p}$ is in the same ray class as $\mathfrak{p}'$, and $\mathfrak{q}$ is in the same ray class as $\mathfrak{q}'$, then $\mathfrak{pq}$ is in the same ray class as $\mathfrak{p}'\mathfrak{q}'$.

  Note that there is no analogue of element addition for the ideals (for instance, $(1) = (-1)$ but $(1) + (1) \neq (1) + (-1)$), so this is the best we can hope for.

  In other words, the ray classes will form an *abelian group* under multiplication, with the operation induced from ideal multiplication.
- For a fixed modulus $\mathfrak{f}$, there are only finitely many ray classes.

In the section above, you may think of a prime ideal $\mathfrak{p} \in \mathcal{O}_K$ as an irreducible factor, such that all ideals can be written as products of. However, they can also naturally be used as a modulus:

**A prime $\mathfrak{p}$ gives a way to divide the elements of $\mathcal{O}_K$ into residue classes that respects the addition and multiplication of elements.**

This can further be generalized to divide up the *ideals* of $\mathcal{O}_K$ into ray classes – unfortunately, using only the finite primes is insufficient to divide up the ideals the way we want, as later seen in Example 63.3.3. So, the infinite primes will be introduced in order to divide up the *elements*, as well as the ideals, into classes that satisfies the multiplicative structure.

## §63.2 Infinite primes

*Prototypical example for this section:* *$\mathbb{Q}(\sqrt{-5})$ has a complex infinite prime, $\mathbb{Q}(\sqrt{5})$ has two real infinite ones.*

Let $K$ be a number field of degree $n$ and signature $(r, s)$. We know what a prime ideal of $\mathcal{O}_K$ is, but we now allow for the so-called infinite primes, which I'll describe using the embeddings.[1] Recall there are $n$ embeddings $\sigma \colon K \to \mathbb{C}$, which consist of

- $r$ real embeddings where $\operatorname{im}\sigma \subseteq \mathbb{R}$, and
- $s$ pairs of conjugate complex embeddings.

Hence $r + 2s = n$. The first class of embeddings form the **real infinite primes**, while the **complex infinite primes** are the second type. We say $K$ is **totally real** (resp **totally complex**) if all its infinite primes are real (resp complex).

**Example 63.2.1** (Examples of infinite primes)

- $\mathbb{Q}$ has a single real infinite prime. We often write it as $\infty$.
- $\mathbb{Q}(\sqrt{-5})$ has a single complex infinite prime, and no real infinite primes. Hence totally complex.
- $\mathbb{Q}(\sqrt{5})$ has two real infinite primes, and no complex infinite primes. Hence totally real.

## §63.3 Modular arithmetic with infinite primes

A **modulus** (or **module**) of $K$ is a formal product

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

where the product runs over all primes, finite and infinite. (Here $\nu(\mathfrak{p})$ is a nonnegative integer, of which only finitely many are nonzero.) We also require that

- $\nu(\mathfrak{p}) = 0$ for any complex infinite prime $\mathfrak{p}$, and
- $\nu(\mathfrak{p}) \le 1$ for any real infinite prime $\mathfrak{p}$.

[1] This is not really the right definition; the "correct" way to think of primes, finite or infinite, is in terms of valuations. But it'll be sufficient for me to state the theorems I want.

Obviously, every $\mathfrak{m}$ can be written as $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ by separating the finite from the (real) infinite primes.

We say $a \equiv b \pmod{\mathfrak{p}}$ if

- If $\mathfrak{p}$ is a finite prime, then $a \equiv b \pmod{\mathfrak{p}^{\nu(\mathfrak{p})}}$ means exactly what you think it should mean: $a - b \in \mathfrak{p}^{\nu(\mathfrak{p})}$.
- If $\mathfrak{p}$ is a *real* infinite prime $\sigma \colon K \to \mathbb{R}$, then $a \equiv b \pmod{\mathfrak{p}}$ means that $\sigma(a/b) > 0$.

**A real infinite prime $\mathfrak{p} = \sigma$ divides up the elements of $K^\times$ into two classes $\{k \in K^\times \mid \sigma(k) > 0\}$ and $\{k \in K^\times \mid \sigma(k) < 0\}$, this division satisfies the multiplicative operation.**

Of course, $a \equiv b \pmod{\mathfrak{m}}$ means $a \equiv b$ modulo each prime power in $\mathfrak{m}$. With this, we can define a generalization of the class group:

**Definition 63.3.1.** Let $\mathfrak{m}$ be a modulus of a number field $K$.

- Let $I_K(\mathfrak{m})$ denote the set of all fractional ideals of $K$ which are relatively prime to $\mathfrak{m}$, which is an abelian group.
- Let $P_K(\mathfrak{m})$ be the subgroup of $I_K(\mathfrak{m})$ generated by
$$\left\{\alpha\mathcal{O}_K \mid \alpha \in K^\times \text{ and } \alpha \equiv 1 \pmod{\mathfrak{m}}\right\}.$$
This is sometimes called a "ray" of principal ideals.[2]

Finally define the **ray class group** of $\mathfrak{m}$ to be $C_K(\mathfrak{m}) = I_K(\mathfrak{m})/P_K(\mathfrak{m})$.

This group is known to always be finite. Note the usual class group is $C_K(1)$.

One last definition that we'll use right after Artin reciprocity:

**Definition 63.3.2.** A **congruence subgroup** of $\mathfrak{m}$ is a subgroup $H$ with
$$P_K(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m}).$$

Thus $C_K(\mathfrak{m})$ is a group which contains a lattice of various quotients $I_K(\mathfrak{m})/H$, where $H$ is a congruence subgroup.

This definition takes a while to get used to, so here are examples.

**Example 63.3.3** (Ray class groups in $\mathbb{Q}$, finite modulus)
Consider $K = \mathbb{Q}$ with infinite prime $\infty$. Then

- If we take $\mathfrak{m} = 1$ then $I_{\mathbb{Q}}(1)$ is all fractional ideals, and $P_{\mathbb{Q}}(1)$ is all principal fractional ideals. Their quotient is the usual class group of $\mathbb{Q}$, which is trivial.
- Now take $\mathfrak{m} = 8$. Thus $I_{\mathbb{Q}}(8) \cong \{\frac{a}{b}\mathbb{Z} \mid a/b \equiv 1, 3, 5, 7 \pmod 8\}$. Moreover
$$P_{\mathbb{Q}}(8) \cong \left\{\frac{a}{b}\mathbb{Z} \mid a/b \equiv 1 \pmod 8\right\}.$$
You might at first glance think that the quotient is thus $(\mathbb{Z}/8\mathbb{Z})^\times$. But the issue is that we are dealing with *ideals*: specifically, we have
$$7\mathbb{Z} = -7\mathbb{Z} \in P_{\mathbb{Q}}(8)$$

[2] Probably because, similar to a geometrical ray, it only extends infinitely in one direction – at least when there is an infinite prime in the modulus $\mathfrak{m}$.

because $-7 \equiv 1 \pmod 8$. So *actually*, we get

$$C_{\mathbb{Q}}(8) \cong \{1,3,5,7 \bmod 8\} / \{1,7 \bmod 8\} \cong (\mathbb{Z}/4\mathbb{Z})^\times.$$

More generally,

$$C_{\mathbb{Q}}(m) = (\mathbb{Z}/m\mathbb{Z})^\times / \{\pm 1\}.$$

**Example 63.3.4** (Ray class groups in $\mathbb{Q}$, infinite moduli)

Consider $K = \mathbb{Q}$ with infinite prime $\infty$ again.

- Now take $\mathfrak{m} = \infty$. As before $I_{\mathbb{Q}}(\infty) = \mathbb{Q}^\times$. Now, by definition we have

  $$P_{\mathbb{Q}}(\infty) = \left\{ \frac{a}{b}\mathbb{Z} \mid a/b > 0 \right\}.$$

  At first glance you might think this was $\mathbb{Q}_{>0}$, but the same behavior with ideals shows in fact $P_{\mathbb{Q}}(\infty) = \mathbb{Q}^\times$. So in this case, $P_{\mathbb{Q}}(\infty)$ still has all principal fractional ideals. Therefore, $C_{\mathbb{Q}}(\infty)$ is still trivial.

- Finally, let $\mathfrak{m} = 8\infty$. As before $I_{\mathbb{Q}}(8\infty) \cong \{\frac{a}{b}\mathbb{Z} \mid a/b \equiv 1,3,5,7 \pmod 8\}$. Now in this case:

  $$P_{\mathbb{Q}}(8\infty) \cong \left\{ \frac{a}{b}\mathbb{Z} \mid a/b \equiv 1 \pmod 8 \text{ and } a/b > 0 \right\}.$$

  This time, we really do have $-7\mathbb{Z} \notin P_{\mathbb{Q}}(8\infty)$: we have $7 \not\equiv 1 \pmod 8$ and also $-7 < 0$. So neither of the generators of $7\mathbb{Z}$ are in $P_{\mathbb{Q}}(8\infty)$. Thus we finally obtain

  $$C_{\mathbb{Q}}(8\infty) \cong \{1,3,5,7 \bmod 8\} / \{1 \bmod 8\} \cong (\mathbb{Z}/8\mathbb{Z})^\times$$

  with the bijection $C_{\mathbb{Q}}(8\infty) \to (\mathbb{Z}/8\mathbb{Z})^\times$ given by $a\mathbb{Z} \mapsto |a| \pmod 8$.

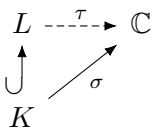
More generally,

$$C_{\mathbb{Q}}(m\infty) = (\mathbb{Z}/m\mathbb{Z})^\times.$$

## §63.4 Infinite primes in extensions

I want to emphasize that everything above is *intrinsic* to a particular number field $K$. After this point we are going to consider extensions $L/K$ but it is important to keep in mind the distinction that the concept of modulus and ray class group are objects defined solely from $K$ rather than the above $L$.

Now take a *Galois* extension $L/K$ of degree $m$. We already know prime ideals $\mathfrak{p}$ of $K$ break into a product of prime ideals $\mathfrak{P}$ of $L$ in a nice way, so we want to do the same thing with infinite primes. This is straightforward: each of the $n$ infinite primes $\sigma\colon K \to \mathbb{C}$ lifts to $m$ infinite primes $\tau\colon L \to \mathbb{C}$, by which I mean the diagram




commutes. Hence like before, each infinite prime $\sigma$ of $K$ has $m$ infinite primes $\tau$ of $L$ which lie above it.

For a real prime $\sigma$ of $K$, if any of the resulting $\tau$ above it are complex, we say that the prime $\sigma$ **ramifies** in the extension $L/K$. Otherwise it is **unramified** in $L/K$. An infinite prime of $K$ is always unramified in $L/K$. In this way, we can talk about an unramified Galois extension $L/K$: it is one where all primes (finite or infinite) are unramified.

**Example 63.4.1** (Ramification of $\infty$)
Let $\infty$ be the real infinite prime of $\mathbb{Q}$.

- $\infty$ is ramified in $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$.
- $\infty$ is unramified in $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$.

Note also that if $K$ is totally complex then any extension $L/K$ is unramified.

## §63.5 Frobenius element and Artin symbol

Recall the key result:

**Theorem 63.5.1** (Frobenius element)
Let $L/K$ be a *Galois* extension. If $\mathfrak{p}$ is a prime unramified in $L/K$, and $\mathfrak{P}$ a prime above it in $L$, then there is a unique element of $\mathrm{Gal}(L/K)$, denoted $\mathrm{Frob}_{\mathfrak{P}}$, obeying

$$\mathrm{Frob}_{\mathfrak{P}}(\alpha) \equiv \alpha^{\mathrm{N}(\mathfrak{p})} \pmod{\mathfrak{P}} \qquad \forall \alpha \in \mathcal{O}_L.$$

Recall some examples from Example 62.1.2 and Lemma 62.4.1.

**Example 63.5.2** (Example of Frobenius elements)
Let $L = \mathbb{Q}(i)$, $K = \mathbb{Q}$. We have $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$.

If $p$ is an odd prime with $\mathfrak{P}$ above it, then $\mathrm{Frob}_{\mathfrak{P}}$ is the unique element such that

$$(a+bi)^p \equiv \mathrm{Frob}_{\mathfrak{P}}(a+bi) \pmod{\mathfrak{P}}$$

in $\mathbb{Z}[i]$. In particular,

$$\mathrm{Frob}_{\mathfrak{P}}(i) = i^p = \begin{cases} i & p \equiv 1 \pmod 4 \\ -i & p \equiv 3 \pmod 4. \end{cases}$$

From this we see that $\mathrm{Frob}_{\mathfrak{P}}$ is the identity when $p \equiv 1 \pmod 4$ and $\mathrm{Frob}_{\mathfrak{P}}$ is complex conjugation when $p \equiv 3 \pmod 4$.

**Example 63.5.3** (Cyclotomic Frobenius element)
Generalizing previous example, let $L = \mathbb{Q}(\zeta)$ and $K = \mathbb{Q}$, with $\zeta$ an $m$th root of unity. It's well-known that $L/K$ is unramified outside $\infty$ and prime factors of $m$. Moreover, the Galois group $\mathrm{Gal}(L/K)$ is $(\mathbb{Z}/m\mathbb{Z})^\times$: the Galois group consists of elements of the form

$$\sigma_n \colon \zeta \mapsto \zeta^n$$

and $\mathrm{Gal}(L/K) = \{\sigma_n \mid n \in (\mathbb{Z}/m\mathbb{Z})^\times\}$.

Then it follows just like before that if $p \nmid m$ is prime and $\mathfrak{P}$ is above $p$

$$\mathrm{Frob}_{\mathfrak{P}}(x) = \sigma_p.$$

Here, as hinted in Section 61.6, we have to generalize the theory where the base field $K$ is not necessarily $\mathbb{Q}$ (for example, in Example 63.5.8, we need $K = \mathbb{Q}(\omega)$). In this case, $\mathfrak{p}$ is not necessarily an integer, and the induced map on the quotient is the "power-by-$\mathrm{N}(\mathfrak{p})$" map.

**Example 63.5.4** (Frobenius element when the base field is $\mathbb{Q}(\omega)$)

Let $L = \mathbb{Q}(\omega, \sqrt[3]{2})$ and $K = \mathbb{Q}(\omega)$.

Consider $\mathfrak{p} = (5)$, which is prime in $K$, and $\mathrm{N}(\mathfrak{p}) = 25$. The field $\mathcal{O}_K/\mathfrak{p}$ is isomorphic to $\mathbb{F}_{25}$. In $L$, $\mathfrak{p}$ splits to $\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$, and each residue field $\mathcal{O}_L/\mathfrak{P}_i$ is isomorphic to $\mathbb{F}_{25}$.

The Frobenius element $\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(L/K)$ induces the power-of-25 isomorphism in the quotient field, thus is the identity.

An important property of the Frobenius element is its order is related to the decomposition of $\mathfrak{p}$ in the higher field $L$ in the nicest way possible:

**Lemma 63.5.5** (Order of the Frobenius element)

The Frobenius element $\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(L/K)$ of an extension $L/K$ has order equal to the inertial degree of $\mathfrak{P}$, that is,

$$\operatorname{ord} \mathrm{Frob}_{\mathfrak{P}} = f(\mathfrak{P} \mid \mathfrak{p}).$$

In particular, $\mathrm{Frob}_{\mathfrak{P}} = \mathrm{id}$ if and only if $\mathfrak{p}$ splits completely in $L/K$.

This naturally generalizes Lemma 62.1.3.

*Proof.* We want to understand the order of the map $T\colon x \mapsto x^{\mathrm{N}(\mathfrak{p})}$ on the field $\mathcal{O}_L/\mathfrak{P}$. But the latter is isomorphic to the splitting field of $X^{\mathrm{N}(\mathfrak{P})} - X$ in $\mathbb{F}_p$, by Galois theory of finite fields. Hence the order is $\log_{\mathrm{N}(\mathfrak{p})}(\mathrm{N}(\mathfrak{P})) = f(\mathfrak{P} \mid \mathfrak{p})$. □

The Galois group acts transitively among the set of $\mathfrak{P}$ above a given $\mathfrak{p}$, so that we have

$$\mathrm{Frob}_{\sigma(\mathfrak{P})} = \sigma \circ (\mathrm{Frob}_{\mathfrak{P}}) \circ \sigma^{-1}.$$

Thus $\mathrm{Frob}_{\mathfrak{P}}$ is determined by its underlying $\mathfrak{p}$ up to conjugation.

In class field theory, we are interested in **abelian extensions**, i.e. those for which $\mathrm{Gal}(L/K)$ is abelian. Here the theory becomes extra nice: the conjugacy classes have size one.

**Definition 63.5.6.** Assume $L/K$ is an **abelian** extension. Then for a given unramified prime $\mathfrak{p}$ in $K$, the element $\mathrm{Frob}_{\mathfrak{P}}$ doesn't depend on the choice of $\mathfrak{P}$. We denote the resulting $\mathrm{Frob}_{\mathfrak{P}}$ by the **Artin symbol**,

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

The definition of the Artin symbol is written deliberately to look like the Legendre symbol. To see why:

**Example 63.5.7** (Legendre symbol subsumed by Artin symbol)

Suppose we want to understand $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}}$ where $p > 2$ is prime. Consider the element

$$\left(\frac{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}{p\mathbb{Z}}\right) \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}).$$

It is uniquely determined by where it sends $\sqrt{2}$. But in fact we have

$$\left(\frac{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}{p\mathbb{Z}}\right)\left(\sqrt{2}\right) \equiv \left(\sqrt{2}\right)^p \equiv 2^{\frac{p-1}{2}} \cdot \sqrt{2} \equiv \left(\frac{2}{p}\right)\sqrt{2} \pmod{\mathfrak{P}}$$

where $\left(\frac{2}{p}\right)$ is the usual Legendre symbol, and $\mathfrak{P}$ is above $p$ in $\mathbb{Q}(\sqrt{2})$. Thus the Artin symbol generalizes the quadratic Legendre symbol.

**Example 63.5.8** (Cubic Legendre symbol subsumed by Artin symbol)

Similarly, it also generalizes the cubic Legendre symbol. To see this, assume $\theta$ is a primary prime in $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$ (thus $\mathcal{O}_K = \mathbb{Z}[\omega]$ is the Eisenstein integers). Then for example

$$\left(\frac{K(\sqrt[3]{2})/K}{\theta\mathcal{O}_K}\right)\left(\sqrt[3]{2}\right) \equiv \left(\sqrt[3]{2}\right)^{\mathrm{N}(\theta)} \equiv 2^{\frac{\mathrm{N}(\theta)-1}{3}} \cdot \sqrt[3]{2} \equiv \left(\frac{2}{\theta}\right)_3 \sqrt[3]{2}. \pmod{\mathfrak{P}}$$

where $\mathfrak{P}$ is above $(\theta)$ in $K(\sqrt[3]{2})$.

## §63.6 Artin reciprocity

Now, we further capitalize on the fact that $\mathrm{Gal}(L/K)$ is abelian. For brevity, in what follows let $\mathrm{Ram}(L/K)$ denote the primes of $K$ (either finite or infinite) which ramify in $L$.

**Definition 63.6.1.** Let $L/K$ be an abelian extension and let $\mathfrak{m}$ be divisible by every prime in $\mathrm{Ram}(L/K)$. Then since $L/K$ is abelian we can extend the Artin symbol multiplicatively to a map

$$\left(\frac{L/K}{\bullet}\right) : I_K(\mathfrak{m}) \twoheadrightarrow \mathrm{Gal}(L/K).$$

This is called the **Artin map**, and it is surjective (for example by Chebotarev Density).

Let $H(L/K, \mathfrak{m}) \subseteq I_K(\mathfrak{m})$ denote the kernel of this map, so

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

We can now present the long-awaited Artin reciprocity theorem.

**Theorem 63.6.2** (Artin reciprocity)

Let $L/K$ be an abelian extension. Then there is a modulus $\mathfrak{f} = \mathfrak{f}(L/K)$, divisible by exactly the primes of $\operatorname{Ram}(L/K)$, such that: for any modulus $\mathfrak{m}$ divisible by all primes of $\operatorname{Ram}(L/K)$, we have

$$P_K(\mathfrak{m}) \subseteq H(L/K, \mathfrak{m}) \subseteq I_K(\mathfrak{m}) \quad \text{if and only if} \quad \mathfrak{f} \mid \mathfrak{m}.$$

We call $\mathfrak{f}$ the **conductor** of $L/K$.

So the conductor $\mathfrak{f}$ plays a similar role to the discriminant (divisible by exactly the primes which ramify), and when $\mathfrak{m}$ is divisible by the conductor, $H(L/K, \mathfrak{m})$ is a *congruence subgroup*.

Here's the reason this is called a "reciprocity" theorem. The above theorem applies on $\mathfrak{m} = \mathfrak{f}$ tells us $P_K(\mathfrak{f}) \subseteq H(L/K, \mathfrak{f})$, so the Artin map factors through the quotient map $I_K(\mathfrak{f}) \twoheadrightarrow I_K(\mathfrak{f})/P_K(\mathfrak{f})$. Recalling that $C_K(\mathfrak{f}) = I_K(\mathfrak{f})/P_K(\mathfrak{f})$, we get a sequence of maps

$$\begin{array}{ccccc} I_K(\mathfrak{f}) & \twoheadrightarrow & C_K(\mathfrak{f}) & \xrightarrow{\left(\frac{L/K}{\bullet}\right)} & \operatorname{Gal}(L/K) \\ & & & \searrow \quad \nearrow_{\cong} & \\ & & & I_K(\mathfrak{f})/H(L/K,\mathfrak{f}) & \end{array}$$

Consequently:

**For primes $\mathfrak{p} \in I_K(\mathfrak{f})$, $\left(\frac{L/K}{\mathfrak{p}}\right)$ depends only on "$\mathfrak{p} \pmod{\mathfrak{f}}$".**

Let's see how this result relates to quadratic reciprocity.

**Example 63.6.3** (Artin reciprocity implies quadratic reciprocity)

The big miracle of quadratic reciprocity states that: for a fixed (squarefree) $a$, the Legendre symbol $\left(\frac{a}{p}\right)$ should only depend the residue of $p$ modulo something. Let's see why Artin reciprocity tells us this *a priori*.

Let $L = \mathbb{Q}(\sqrt{a})$, $K = \mathbb{Q}$. Then we've already seen that the Artin symbol

$$\left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{\bullet}\right)$$

is the correct generalization of the Legendre symbol. Thus, Artin reciprocity tells us that there is a conductor $\mathfrak{f} = \mathfrak{f}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ such that $\left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{p}\right)$ depends only on the residue of $p$ modulo $\mathfrak{f}$, which is what we wanted.

Here is an example along the same lines.

**Example 63.6.4** (Cyclotomic field)

Let $\zeta$ be a primitive $m$th root of unity. For primes $p$, we know that $\operatorname{Frob}_p \in \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is "exactly" $p \pmod{m}$. Let's translate this idea into the notation of Artin reciprocity.

We are going to prove

$$H(\mathbb{Q}(\zeta)/\mathbb{Q}, m\infty) = P_{\mathbb{Q}}(m\infty) = \left\{ \frac{a}{b}\mathbb{Z} \mid a/b \equiv 1 \pmod{m} \right\}.$$

This is the generic example of achieving the lower bound in Artin reciprocity. It also implies that $\mathfrak{f}(\mathbb{Q}(\zeta)/\mathbb{Q}) \mid m\infty$.

It's well-known $\mathbb{Q}(\zeta)/\mathbb{Q}$ is unramified outside finite primes dividing $m$, so that the Artin symbol is defined on $I_K(\mathfrak{m})$. Now the Artin map is given by

$$\begin{array}{ccccc} I_{\mathbb{Q}}(\mathfrak{m}) & \xrightarrow{\left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{\bullet}\right)} & \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) & \xrightarrow{\cong} & (\mathbb{Z}/m\mathbb{Z})^\times \\ p & \longmapsto & (x \mapsto x^p) & \longmapsto & p \pmod{m}. \end{array}$$

So we see that the kernel of this map is trivial, i.e. it is given by the identity of the Galois group, corresponding to $1 \pmod{m}$. On the other hand, we've also computed $P_{\mathbb{Q}}(m\infty)$ already, so we have the desired equality.

In fact, we also have the following "existence theorem": every congruence subgroup appears uniquely once we fix $\mathfrak{m}$.

**Theorem 63.6.5** (Takagi existence theorem)

Fix $K$ and let $\mathfrak{m}$ be a modulus. Consider any congruence subgroup $H$, i.e.

$$P_K(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m}).$$

Then $H = H(L/K, \mathfrak{m})$ for a *unique* abelian extension $L/K$.

Finally, such subgroups reverse inclusion in the best way possible:

**Lemma 63.6.6** (Inclusion-reversing congruence subgroups)

Fix a modulus $\mathfrak{m}$. Let $L/K$ and $M/K$ be abelian extensions and suppose $\mathfrak{m}$ is divisible by the conductors of $L/K$ and $M/K$. Then

$$L \subseteq M \quad \text{if and only if} \quad H(M/K, \mathfrak{m}) \subseteq H(L/K, \mathfrak{m}).$$

Here by $L \subseteq M$ we mean that $L$ is isomorphic to some subfield of $M$.

*Sketch of proof.* Let us first prove the equivalence with $\mathfrak{m}$ fixed. In one direction, assume $L \subseteq M$; one can check from the definitions that the diagram

$$\begin{array}{ccc} I_K(\mathfrak{m}) & \xrightarrow{\left(\frac{M/K}{\bullet}\right)} & \mathrm{Gal}(M/K) \\ & \searrow^{\left(\frac{L/K}{\bullet}\right)} & \downarrow \\ & & \mathrm{Gal}(L/K) \end{array}$$

commutes, because it suffices to verify this for prime powers, which is just saying that Frobenius elements behave well with respect to restriction. Then the inclusion of kernels follows directly. The reverse direction is essentially the Takagi existence theorem. □

Note that we can always take $\mathfrak{m}$ to be the product of conductors here.

If you didn't realize it: Apart from generalizing quadratic reciprocity, Artin reciprocity and Takagi existence theorem together enumerates *all abelian field extensions*! Now if you are given a field $K$ and want to list all (finite) abelian field extensions of $K$, you can list all the modulus $\mathfrak{m}$ of $K$, list all subgroups of $C_K(\mathfrak{m})$, then each subgroup corresponds to a field extension.

(Of course, the question of how to compute the field $L$ given a modulus and a congruence subgroup is still difficult. At least when $K = \mathbb{Q}$, Problem 63A† gives the answer: all finite abelian field extensions $L/\mathbb{Q}$ are contained in some cyclotomic field.

To finish, here is a quote from Emil Artin on his reciprocity law:

> I will tell you a story about the Reciprocity Law. After my thesis, I had the idea to define $L$-series for non-abelian extensions. But for them to agree with the $L$-series for abelian extensions, a certain isomorphism had to be true. I could show it implied all the standard reciprocity laws. So I called it the General Reciprocity Law and tried to prove it but couldn't, even after many tries. Then I showed it to the other number theorists, but they all laughed at it, and I remember Hasse in particular telling me it couldn't possibly be true.
>
> Still, I kept at it, but nothing I tried worked. Not a week went by — *for three years!* — that I did not try to prove the Reciprocity Law. It was discouraging, and meanwhile I turned to other things. Then one afternoon I had nothing special to do, so I said, 'Well, I try to prove the Reciprocity Law again.' So I went out and sat down in the garden. You see, from the very beginning I had the idea to use the cyclotomic fields, but they never worked, and now I suddenly saw that all this time I had been using them in the wrong way — and in half an hour I had it.

## §63.7 Application: Generalization of sum of two squares

We start with the follow classical theorem:

**Theorem 63.7.1** (Fermat's theorem on sums of two squares)
An odd prime $p$ can be expressed as $p = x^2 + y^2$ for integers $x$ and $y$ if and only if $p \equiv 1 \pmod 4$.

You may see a proof that goes something like the following. Because we have learnt number theory and quadratic reciprocity, this should be intuitive to follow.

*Proof.* Note that if $p = x^2 + y^2$, then $\left(\frac{x}{y}\right)^2 \equiv -1 \pmod p$, so a necessary condition is that $-1$ is a quadratic residue modulo $p$.

We will show that this condition is also sufficient.

Let $a \in \mathbb{Z}$ be such that $a^2 \equiv -1 \pmod p$. Note that $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(a+i) = a^2+1$ is divisible by $p$, and $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(p) = p^2$.

Assume it is possible to write $p = x^2 + y^2$. Then $p$ can be factored in $\mathbb{Z}[i]$ as $(x + yi)(x - yi)$, for integers $x$ and $y$.

We claim that letting $x + yi = \gcd(p, a + i)$ works. Indeed, $p \mid (a + i)(a - i) = a^2 + 1$ but $p$ does not divide either of the factor, which means $p$ is not a prime in $\mathbb{Z}[i]$ and taking the gcd with either $a + i$ or $a - i$ should extract a nontrivial factor.

Note that $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(x+yi) = p$, thus $x+yi$ and $x-yi$ are already primes, so the factor extraction above must already give us a prime factor, which is what we want.

Finally, we know that $-1$ is a quadratic residue modulo $p$ precisely when $p \equiv 1 \pmod 4$, so we're done. □

You may dismiss it as an arcane trick... until you realize that it can be generalized perfectly well to many other cases! Try to prove the following theorem using the same method.

**Theorem 63.7.2**

An odd prime $p > 7$ can be expressed as $p = x^2 + 7y^2$ for integers $x$ and $y$ if and only if $-7$ is a quadratic residue modulo $p$.

Which, by quadratic reciprocity, would boil down to whether $(p \bmod 7) \in \{1, 2, 4\}$.

Nevertheless, it isn't always that nice.

**Example 63.7.3**

Let $p = 3$. Then $1^2 \equiv -5 \pmod p$, but there is no integers $x$ and $y$ such that $p = x^2 + 5y^2$.

**Question 63.7.4.** If you haven't, try to figure out what went wrong in the proof before reading the explanation below.

The bug, of course, is to assume that $\gcd(p, 1+\sqrt{-5})$ is an element — that is, in this case, the ring of integers of $\mathbb{Q}(\sqrt{-5})$ is not an unique factorization domain. But we have all the tools of ideal theory to fix it: the ideal $(p) = (3) \subseteq \mathbb{Q}$ splits into $(p) = \mathfrak{p}_1\mathfrak{p}_2$ when lifted to $\mathbb{Q}(\sqrt{-5})$, where $\mathfrak{p}_1 = (3, 1+\sqrt{-5})$ and $\mathfrak{p}_2 = (3, 1-\sqrt{-5})$.

Thus,

**Proposition 63.7.5**

A prime $p \in \mathbb{Q}$ can be written as $p = x^2 + 5y^2$ if and only if $(p)$ splits into $\mathfrak{p}_1\mathfrak{p}_2$ when lifted to $\mathbb{Q}(\sqrt{-5})$, where both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are principal ideals.

This is where Artin reciprocity and the Hilbert class field shines — we want to determine the class of $\mathfrak{p}_1$, in other words, $\mathfrak{p}_1 \pmod 1$.

**Question 63.7.6.** Check that $\mathfrak{p} \equiv (1) \pmod 1$ if and only if $\mathfrak{p} \subseteq \mathbb{Q}(\sqrt{-5})$ is principal. (Definition chasing.)

**Question 63.7.7.** If $\mathfrak{p}_1$ is principal, then we automatically have $\mathfrak{p}_2$ principal. Why?

From now on, let $K = \mathbb{Q}(\sqrt{-5})$, and let $L$ be some abelian extension of $K$.

Recall we defined above the group $H(L/K, \mathfrak{m}) = \ker\left(\frac{L/K}{\bullet}\right)$, and the statement of Artin reciprocity claims, among others, that $P_K(\mathfrak{m}) \subseteq H(L/K, \mathfrak{m})$. Naturally, you may wonder, if all we cares is that "$\left(\frac{L/K}{\mathfrak{p}}\right)$ depends only on $\mathfrak{p} \pmod{\mathfrak{f}}$", then why would we need to define yet another piece of notation for $H$?

Well, the simplified version of Artin reciprocity theorem above states that we can compute $\left(\frac{L/K}{\mathfrak{p}}\right)$ once we know $\mathfrak{p} \pmod{\mathfrak{f}}$. Of course there is more than that:

**If $P_K(\mathfrak{f}) = H(L/K, \mathfrak{f})$, then we can compute $\mathfrak{p} \pmod{\mathfrak{f}}$ once we know $\left(\frac{L/K}{\mathfrak{p}}\right)$.**

In other words, if $L$ is such that the congruence subgroup reaches the "lower bound", then we also get the converse.

**Question 63.7.8.** Check that the algebra above works out.

We have seen one example above, Example 63.6.4, where the congruence subgroup $H(\mathbb{Q}(\zeta_m)/\mathbb{Q}, m\infty)$ is equal to the lower bound $P_{\mathbb{Q}}(m\infty)$. We will see one more example below.

### Example 63.7.9

In the example above, we can vary both the modulus $\mathfrak{m}$ and the abelian field extension $L$ over $K$ to get different congruence subgroups. This can be confusing, so let us take an example.

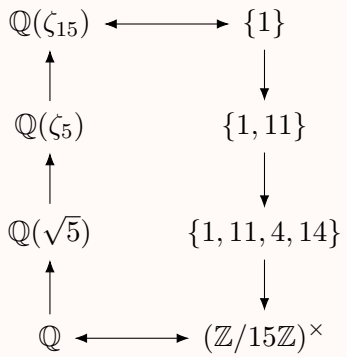
Consider abelian field extensions $L/\mathbb{Q}$. Let the modulus in $\mathbb{Q}$ be $\mathfrak{m} = 15\infty$.

The ray class group $C_K(\mathfrak{m})$ is of course isomorphic to $(\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

As small as this group is (with only 8 elements), it has 8 subgroups.[a] Nevertheless, we will only focus on the relevant parts of the subgroup lattice.

By Artin reciprocity and Takagi existence theorem, each congruence subgroup corresponds to some abelian extension over $L/\mathbb{Q}$.

We draw the correspondence between abelian field extension and the congruence subgroup $H(L/\mathbb{Q}, 15\infty)$ below, depicted using the fact that $H(L/\mathbb{Q}, 15\infty)/P_{\mathbb{Q}}(15\infty)$ is a subgroup of $C_{\mathbb{Q}}(15\infty)$, which is canonically isomorphic to $(\mathbb{Z}/15\mathbb{Z})^\times$.




(Where does the diagram above come from? Well, if the base field is $\mathbb{Q}$, Problem 63A† gives a way.)

Interested readers may want to try to work out the canonical isomorphism between the Galois group $\mathrm{Gal}(L/K)$ and the ray class group $C_K(\mathfrak{f}(L/K))$ in the general case of an abelian extension.

Next, how does this relate to the abelian extensions that corresponds to different modulus, let's say $5\infty$? Intuitively speaking, if we know the value of an ideal mod $15\infty$, we would know its value mod $5\infty$. Formally, we have this diagram:

$$\begin{array}{ccccc} P_K(15\infty) & \hookrightarrow & I_K(15\infty) & \twoheadrightarrow & C_K(15\infty) \\ \downarrow & & \downarrow & & \downarrow \\ P_K(5\infty) & \hookrightarrow & I_K(5\infty) & \twoheadrightarrow & C_K(5\infty) \end{array}$$

(If you have read the category theory chapter: Morphism of short exact sequence appears everywhere! You just have to look for it.)

That is, we get an induced $C_K(15\infty) \twoheadrightarrow C_K(5\infty)$ map, or equivalently, $(\mathbb{Z}/15\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/5\mathbb{Z})^\times$. This time around, the abelian field extensions that corresponds to the modulus $5\infty$ are:

$$\begin{array}{ccc} \mathbb{Q}(\zeta_5) & \longleftrightarrow & \{1\} \\ \uparrow & & \downarrow \\ \mathbb{Q}(\sqrt{5}) & & \{1,4\} \\ \uparrow & & \downarrow \\ \mathbb{Q} & \longleftrightarrow & (\mathbb{Z}/5\mathbb{Z})^\times \end{array}$$

[a] https://beta.lmfdb.org/Groups/Abstract/diagram/8.2 has a diagram.

In our case, given $p \in \mathbb{Q}$ be a prime factors as $(p) = \mathfrak{p}_1\mathfrak{p}_2$ when lifted to $K = \mathbb{Q}(\sqrt{-5})$, we want to determine if $\mathfrak{p}_1$ is principal — in other words, we want to compute "$\mathfrak{p}_1 \pmod 1$". With the insight above, we will rephrase the condition in terms of the Artin symbol.

Let $L = K(i)$. (Later on, we will know that $L$ is the **Hilbert class field** of $K$.) We claim the following is true:

- $L/K$ is an abelian extension,
- the discriminant is $\mathfrak{f} = \mathfrak{f}(L/K) = 1$,
- $H(L/K, \mathfrak{f}) = P_K(\mathfrak{f})$ — that is, this is exactly the situation where we can determine $\mathfrak{p} \pmod 1$ for $\mathfrak{p} \subseteq K$ based on $\left(\frac{L/K}{\mathfrak{p}}\right)$.

(In the general case, the field $L$ exists according to Problem 63B†.)

Then, for a prime $\mathfrak{p} \subseteq K$, the following are equivalent:

1. $\mathfrak{p}$ is principal;
2. $\left(\frac{L/K}{\mathfrak{p}}\right) = \mathrm{id}$;
3. $\mathfrak{p}$ splits completely when lifted to $L$.

Notice that we used Artin reciprocity (and its "converse") for the abelian extension $L/K$ to prove the equivalence of the first and the second statement.

**Exercise 63.7.10.** Why is the second and the third statement equivalent? (Problem 63B†.)

Thus, the condition that $(p) = \mathfrak{p}_1\mathfrak{p}_2$ for principal ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ is equivalent to that $(p) \subseteq \mathbb{Q}$ splits completely when lifted to $L$.

Reasoning similar to above for the abelian extension $L/\mathbb{Q}$, the following are equivalent:

1. $(p) \subseteq \mathbb{Q}$ splits completely when lifted to $L$;

2. $\left(\frac{L/\mathbb{Q}}{(p)}\right) = \mathrm{id}$.

This time, we don't have the first bullet point anymore — $L$ is *not* the Hilbert class field of $\mathbb{Q}$ — but, by Artin reciprocity, we do know:

**The value of $\left(\frac{L/\mathbb{Q}}{(p)}\right)$ only depends on $(p) \pmod{\mathfrak{f}(L/\mathbb{Q})}$.**

In this case, the discriminant of the extension $L/\mathbb{Q}$ is $\mathfrak{f}(L/\mathbb{Q}) = 20\infty$.

So, in summary:

$$\begin{aligned}
&p \text{ can be written as } x^2+5y^2 \\
\iff &(p) = \mathfrak{p}_1\mathfrak{p}_2 \text{ for principal } \mathfrak{p}_1 \text{ when lifted to } \mathbb{Q}(\sqrt{-5}) \\
\iff &(p) = \mathfrak{p}_1\mathfrak{p}_2, \text{ and } \mathfrak{p}_1 \subseteq \mathbb{Q}(\sqrt{-5}) \text{ splits completely when lifted to } \mathbb{Q}(\sqrt{-5}, i) \\
\iff &(p) \subseteq \mathbb{Q} \text{ splits completely when lifted to } \mathbb{Q}(\sqrt{-5}, i) \\
\iff &\left(\frac{\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}}{(p)}\right) = \mathrm{id} \\
\iff &(p \bmod 20) \in \{1, 9\}.
\end{aligned}$$

We're done! The final form of the theorem is:

**Theorem 63.7.11**

Let $p$ be a prime with $p \nmid 20$, then $p$ can be written as $x^2+5y^2$ if and only if $(p \bmod 20) \in \{1, 9\}$.

## §63.8 A few harder problems to think about

**Problem 63A$^\dagger$.** [Kronecker-Weber theorem] Let $L$ be an abelian extension of $\mathbb{Q}$. Then $L$ is contained in a cyclic extension $\mathbb{Q}(\zeta)$ where $\zeta$ is an $m$th root of unity (for some $m$).

**Problem 63B$^\dagger$** (Hilbert class field)**.** Let $K$ be any number field. Then there exists a unique abelian extension $E/K$ which is unramified at all primes (finite or infinite) and such that

- $E/K$ is the maximal such extension by inclusion.
- $\mathrm{Gal}(E/K)$ is isomorphic to the class group of $K$.
- A prime $\mathfrak{p}$ of $K$ splits completely in $E$ if and only if it is a principal ideal of $\mathcal{O}_K$.

We call $E$ the **Hilbert class field** of $K$.

**Problem 63C.** There is no positive integer $m$ such that whether a prime number $p \nmid m$ can be written as $p = x^2+23y^2$ depends only on $p \bmod m$. Guess why.