Algebraic Number Theory, a Computational Approach

William Stein

May 19, 2019

Chapter 1

Decomposition and Inertia Groups

In this chapter we will study extra structure in the case when K is Galois over $\mathbb{Q}$. We will learn about Frobenius elements, the Artin symbol, decomposition groups, and how the Galois group of K is related to Galois groups of residue class fields. These are the basic structures needed to attach L-functions to representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, which will play a central role in the next few chapters.

1.1 Galois Extensions

In this section we give a survey (no proofs) of the basic facts about Galois extensions that will be needed in the rest of this chapter.

Definition 1.1.1 (Galois)**.** An extension L/K of number fields is *Galois* if

$$\#\,\mathrm{Aut}(L/K) = [L : K],$$

where $\mathrm{Aut}(L/K)$ is the group of automorphisms of K that fix L. We write

$$\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K).$$

For example, if $K \subset \mathbb{C}$ is a number field embedded in the complex numbers, then K is *Galois* over $\mathbb{Q}$ if every field homomorphism $K \to \mathbb{C}$ has image K. As another example, any quadratic extension L/K is Galois over K, since it is of the form $K(\sqrt{a})$, for some $a \in K$, and the nontrivial automorphism is induced by $\sqrt{a} \mapsto -\sqrt{a}$, so there is always one nontrivial automorphism. If $f \in K[x]$ is an irreducible cubic polynomial, and α is a root of f, then one proves in a course on Galois theory that $K(\alpha)$ is Galois over K if and only if the discriminant of f is a perfect square in K. "Random" number fields of degree bigger than 2 are rarely Galois.

If $K \subset \mathbb{C}$ is a number field, then the *Galois closure* $\overline{K}$ of K in $\mathbb{C}$ is the field generated by all images of K under all embeddings in $\mathbb{C}$ (more generally, if L/K is an extension, the Galois closure of L over K is the field generated by images of embeddings $L \to \mathbb{C}$ that are the identity map on K).

Exercise 1.1.2. Suppose $K \subset \mathbb{C}$ is a number field of the form $\mathbb{Q}(\alpha)$ for some $\alpha \in \mathbb{C}$. Show that $\overline{K}$ is generated (as an extension of $\mathbb{Q}$) by all the conjugates of α.

How much bigger can the degree of $\overline{K}$ be as compared to the degree of $K = \mathbb{Q}(\alpha)$? There is an embedding of $\mathrm{Gal}(\overline{K}/\mathbb{Q})$ into the group of permutations of the conjugates of α. If α has n conjugates, then this is an embedding $\mathrm{Gal}(\overline{K}/\mathbb{Q}) \hookrightarrow S_n$, where S_n is the symmetric group on n symbols, which has order $n!$. Thus the degree of the $\overline{K}$ over $\mathbb{Q}$ is a divisor of $n!$. Also $\mathrm{Gal}(\overline{K}/\mathbb{Q})$ is a transitive subgroup of S_n, which constrains the possibilities further. When $n = 2$, we recover the fact that quadratic extensions are Galois. When $n = 3$, we see that the Galois closure of a cubic extension is either the cubic extension or a quadratic extension of the cubic extension. One can show that the Galois closure of a cubic extension is obtained by adjoining the square root of the discriminant, which is why an irreducible cubic defines a Galois extension if and only if the discriminant is a perfect square.

For an extension K of $\mathbb{Q}$ of degree 5, it is "frequently" the case that the Galois closure has degree 120, and in fact it is an interesting problem to enumerate examples of degree 5 extensions in which the Galois closure has degree smaller than 120. For example, the only possibilities for the order of a transitive proper subgroup of S_5 are 5, 10, 20, and 60; there are also proper subgroups of S_5 order $2, 3, 4, 6, 8, 12$, and 24, but none are transitive.

Exercise 1.1.3. Let α be a root of the irreducible polynomial $f(x) = x^5 - 6x + 3$ and let $K = \mathbb{Q}(\alpha)$.

1. Use `Sage` to verify that the Galois group $\mathrm{Gal}(\overline{K}/\mathbb{Q})$ has order 120. Warning: this command may take a long time to run. Try to finish the second part of this exercise before your code finishes.

2. One can show that f has three real roots and two complex roots. Show that $\mathrm{Gal}(\overline{K}/\mathbb{Q})$ contains an element of order 5 and an element of order 5. Use this to argue that $\mathrm{Gal}(\overline{K})/\mathbb{Q}$ has order 120.

[*Hint*: Number fields in `Sage` have a `galois_closure()` command that returns the Galois closure of the field. For the second part, you want to show that any 5-cycle and transposition will generate S_5.]

Example 1.1.4. Let n be a positive integer. Consider the field $K = \mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{2\pi i/n}$ is a primitive nth root of unity. If $\sigma : K \to \mathbb{C}$ is an embedding, then $\sigma(\zeta_n)$ is also an nth root of unity, and the group of nth roots of unity is cyclic. So $\sigma(\zeta_n) = \zeta_n^m$ for some m which is invertible modulo n. Thus K is Galois and $\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$. However, $[K : \mathbb{Q}] = \varphi(n)$, so this map is an isomorphism.

Remark 1.1.5. Taking a limit using the maps $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$, we obtain a homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_p^*$, which is called the *$p$-adic cyclotomic character*.

Compositums of Galois extensions are Galois. For example, the biquadratic field $K = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$ is a Galois extension of $\mathbb{Q}$ of degree 4, which is the compositum of the Galois extensions $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-1})$ of $\mathbb{Q}$.

Fix a number field K that is Galois over $\mathbb{Q}$. Then the Galois group acts on many of the objects that we have associated to K.

Exercise 1.1.6. Let L/K be a Galois extension of number fields, and let $G = \mathrm{Gal}(L/K)$. Describe the natural action of G on the following objects:

- The ring of integers $\mathcal{O}_K$.
- The group units U_K.
- The set of ideals of $\mathcal{O}_K$.
- The group of fractional ideals of $\mathcal{O}_K$.
- The class group $\mathrm{Cl}(K)$.
- The set $S_\mathfrak{p}$ of prime ideals of $\mathcal{O}_L$ lying over a given nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, i.e., the prime divisors of $\mathfrak{p}\mathcal{O}_L$.

In the next section we will be concerned with the action of $\mathrm{Gal}(L/K)$ on $S_\mathfrak{p}$, though actions on each of the other objects, especially $\mathrm{Cl}(L)$, are also of great interest. Understanding the action of $\mathrm{Gal}(L/K)$ on $S_\mathfrak{p}$ will enable us to associate, in a natural way, a holomorphic L-function to any complex representation $\mathrm{Gal}(L/K) \to \mathrm{GL}_n(\mathbb{C})$.

1.2 Decomposition of Primes: $efg = n$

Let L/K be an extension of number fields and let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$. By Theorem **??** the ideal $\mathfrak{p}\mathcal{O}_L$ factors uniquely into a product of primes of $\mathcal{O}_L$ given by

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

where the $\mathfrak{q}_i$ are the prime ideals of $\mathcal{O}_L$ laying over $\mathfrak{p}$, and the e_i are positive integers. The goal of this section is to study this factorization. First we will introduce some standard terminology.

Definition 1.2.1 (Ramification Index)**.** The *ramification index* of $\mathfrak{q}_i$ over $\mathfrak{p}$ is

$$e(\mathfrak{P}_i/\mathfrak{p}) = e_i.$$

Definition 1.2.2 (Inertia degree)**.** The *inertia degree* of $\mathfrak{P}_i$ over $\mathfrak{p}$ is

$$f(\mathfrak{P}_i/\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}].$$

Exercise 1.2.3. The following properties follow quickly from the definitions. Let $M/L/K$ be a tower of number fields. Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$, $\mathfrak{q}$ a prime in $\mathcal{O}_L$ lying over $\mathfrak{p}$, and $\mathfrak{P}$ a prime in $\mathcal{O}_M$ lying over $\mathfrak{q}$.

(a) Show that $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{q}) \cdot e(\mathfrak{q}/\mathfrak{p})$.

(b) Show that $f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{q}) \cdot f(\mathfrak{q}/\mathfrak{p})$.

(c) Let $g_{L/K}(\mathfrak{p})$, $g_{M/K}(\mathfrak{p})$ be the number of primes of $\mathcal{O}_L$, $\mathcal{O}_M$ lying over $\mathfrak{p}$ respectively. Show that

$$g_{M/K}(\mathfrak{p}) = \sum_{\mathfrak{q} \text{ divides } \mathfrak{p}\mathcal{O}_L} g_{L/K}(\mathfrak{q}).$$

Now suppose that L/K is Galois and let $\sigma \in \mathrm{Gal}(L/K)$. We saw in Exercise 1.1.6 that $\mathrm{Gal}(L/K)$ acts naturally on the set $S_\mathfrak{p}$ for a prime $\mathfrak{p}$ of $\mathcal{O}_K$. This means that $\sigma(\mathfrak{P}) \in S_\mathfrak{p}$ for any $\mathfrak{P} \in S_\mathfrak{p}$. Moreover, σ induces an isomorphism of finite fields $\mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\sigma(\mathfrak{P})$ that fixes the common subfield $\mathcal{O}_K/\mathfrak{p}$. Thus $\mathfrak{P}$ and $\sigma(\mathfrak{P})$ have the same inertia degree, i.e. $f(\mathfrak{P}/\mathfrak{p}) = f(\sigma(\mathfrak{P})/\mathfrak{p})$. In fact, much more is true.

Theorem 1.2.4. *Suppose L/K is a Galois extension of number fields, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Write $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$, and let $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. Then $G = \mathrm{Gal}(L/K)$ acts transitively on the set $S_{\mathfrak{p}}$ of primes $\mathfrak{P}_i$, and*

$$e_1 = \cdots = e_g, \qquad f_1 = \cdots = f_g.$$

Moreover, if we let e be the common value of the e_i, f the common value of the f_i, and $n = [K : L]$, then

$$efg = n.$$

Proof. For simplicity, we will give the proof only for an extension $K/\mathbb{Q}$, but the proof works in general. Suppose $p \in \mathbb{Z}$ and $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, and $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_g\}$. We will first prove that $G = \mathrm{Gal}(K/\mathbb{Q})$ acts transitively on S. Let $\mathfrak{p} = \mathfrak{p}_i$ for some i. Recall Lemma **??** which we proved long ago using the Chinese Remainder Theorem (Theorem **??**). It showed there exists $a \in \mathfrak{p}$ such that $(a)/\mathfrak{p}$ is an integral ideal that is coprime to $p\mathcal{O}_K$. The product

$$I = \prod_{\sigma \in G} \sigma((a)/\mathfrak{p}) = \prod_{\sigma \in G} \frac{(\sigma(a))\mathcal{O}_K}{\sigma(\mathfrak{p})} = \frac{(\mathrm{Norm}_{K/\mathbb{Q}}(a))\mathcal{O}_K}{\prod_{\sigma \in G} \sigma(\mathfrak{p})} \tag{1.1}$$

is a nonzero integral $\mathcal{O}_K$ ideal since it is a product of nonzero integral $\mathcal{O}_K$ ideals. Since $a \in \mathfrak{p}$ we have that $\mathrm{Norm}_{K/\mathbb{Q}}(a) \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Thus the numerator of the rightmost expression in (1.1) is divisible by $p\mathcal{O}_K$. Also, because $(a)/\mathfrak{p}$ is coprime to $p\mathcal{O}_K$, each $\sigma((a)/\mathfrak{p})$ is coprime to $p\mathcal{O}_K$ as well. Thus I is coprime to $p\mathcal{O}_K$. This means the denominator of the rightmost expression in (1.1) must also be divisible by $p\mathcal{O}_K$ in order to cancel the $p\mathcal{O}_K$ in the numerator. Thus we have shown that for any i,

$$\prod_{j=1}^{g} \mathfrak{p}_j^{e_j} = p\mathcal{O}_K \;\Big|\; \prod_{\sigma \in G} \sigma(\mathfrak{p}_i).$$

By unique factorization, since every $\mathfrak{p}_j$ appears in the left hand side, we must have that for each j there is a σ with $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$, i.e., G acts transitively on S.

Choose some j and suppose that $k \neq j$ is another index. Because G acts transitively, there exists $\sigma \in G$ such that $\sigma(\mathfrak{p}_k) = \mathfrak{p}_j$. Applying σ to the factorization $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$, we see that

$$\prod_{i=1}^{g} \mathfrak{p}_i^{e_i} = \prod_{i=1}^{g} \sigma(\mathfrak{p}_i)^{e_i}.$$

Using unique factorization, we get $e_j = e_k$. Thus $e_1 = e_2 = \cdots = e_g$.

As was mentioned right before the statement of the theorem, for any $\sigma \in G$ we have $\mathcal{O}_K/\mathfrak{p}_i \cong \mathcal{O}_K/\sigma(\mathfrak{p}_i)$. Since G acts transitively it follows that $f_1 = f_2 = \cdots = f_g$. We have, upon applying the Chinese Remainder Theorem and noting $\#(\mathcal{O}_K/(\mathfrak{p}^m)) = \#(\mathcal{O}_K/\mathfrak{p})^m$ (see Exercise **??**), that

$$\begin{aligned}[K:\mathbb{Q}] &= \dim_{\mathbb{Z}} \mathcal{O}_K = \dim_{\mathbb{F}_p} \mathcal{O}_K/p\mathcal{O}_K \\ &= \dim_{\mathbb{F}_p}\left(\bigoplus_{i=1}^{g} \mathcal{O}_K/\mathfrak{p}_i^{e_i}\right) = \sum_{i=1}^{g} e_i f_i = efg,\end{aligned}$$

which completes the proof. □

1.2.1 Examples

This section gives examples illustrating the theorem for quadratic fields and a cubic field and its Galois closure.

Quadratic Extensions

Suppose $K/\mathbb{Q}$ is a quadratic field. Then K is Galois, so for each prime $p \in \mathbb{Z}$ we have $2 = efg$. There are exactly three possibilities for e, f and g :

(Ramified): $e = 2$, $f = g = 1$: The prime p *ramifies* in $\mathcal{O}_K$, which means $p\mathcal{O}_K = \mathfrak{p}^2$. Let α be a generator for $\mathcal{O}_K$ and $h \in \mathbb{Z}[x]$ a minimal polynomial for α. By Theorem **??** a prime p is ramified in $\mathcal{O}_K$ if and only if h has a double root modulo p, which is equivalent to p dividing the discriminant of h. This shows there are only finitely many ramified primes.

(Inert): $e = 1$, $f = 2$, $g = 1$: The prime p is *inert* in $\mathcal{O}_K$, which means $p\mathcal{O}_K = \mathfrak{p}$ is prime. It is a nontrivial theorem that this happens half of the time, as we will see illustrated below for a particular example.

(Split): $e = f = 1$, $g = 2$: The prime p *splits* in $\mathcal{O}_K$, which means $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$. This happens the other half of the time.

Example 1.2.5. Let $K = \mathbb{Q}(\sqrt{5})$, so $\mathcal{O}_K = \mathbb{Z}[\gamma]$, where $\gamma = (1+\sqrt{5})/2$. Then $p = 5$ is ramified, since $5\mathcal{O}_K = (\sqrt{5})^2$. More generally, the order $\mathbb{Z}[\sqrt{5}]$ has index 2 in $\mathcal{O}_K$, so for any prime $p \neq 2$ we can determine the factorization of p in $\mathcal{O}_K$ by finding the factorization of the polynomial $x^2 - 5 \in \mathbb{F}_p[x]$. The polynomial $x^2 - 5$ splits as a product of two distinct factors in $\mathbb{F}_p[x]$ if and only if $e = f = 1$ and $g = 2$. For $p \neq 2, 5$ this is the case if and only if 5 is a square in $\mathbb{F}_p$, i.e., if $\left(\frac{5}{p}\right) = 1$, where $\left(\frac{5}{p}\right)$ is $+1$ if 5 is a square mod p and -1 if 5 is not. By quadratic reciprocity,

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}} \cdot \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod 5 \\ -1 & \text{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

Thus whether p splits or is inert in $\mathcal{O}_K$ is determined by the residue class of p modulo 5. It is a theorem of Dirichlet, which was massively generalized by Chebotarev, that $p \equiv \pm 1$ half the time and $p \equiv \pm 2$ the other half the time.[1]

The Cube Root of Two

Suppose $K/\mathbb{Q}$ is not Galois. Then e_i, f_i, and g are defined for each prime $p \in \mathbb{Z}$, but we need not have $e_1 = \cdots = e_g$ or $f_1 = \cdots = f_g$. We do still have that $\sum_{i=1}^{g} e_i f_i = n$, by the Chinese Remainder Theorem as used in the proof of Theorem 1.2.4.

Consider the case where $K = \mathbb{Q}(\sqrt[3]{2})$. We know that $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. Thus $2\mathcal{O}_K = (\sqrt[3]{2})^3$, so for 2 we have $e = 3$ and $f = g = 1$.

Working modulo 5 we have

$$x^3 - 2 = (x+2)(x^2 + 3x + 4) \in \mathbb{F}_5[x],$$

and the quadratic factor is irreducible. Thus

$$5\mathcal{O}_K = \left(5, \sqrt[3]{2} + 2\right) \cdot \left(5, \left(\sqrt[3]{2}\right)^2 + 3\sqrt[3]{2} + 4\right).$$

Thus here $g = 2$, $e_1 = e_2 = 1$, $f_1 = 1$, and $f_2 = 2$. Thus when K is not Galois we need not have that the f_i are all equal.

1.2.2 Definitions and Terminology

In the previous sections we used words like "ramify", "inert", and "split" to describe the decomposition of a prime in an extension. This section will define these terms which will be used in later sections.

Let L/K be an extension of number fields of degree n, and let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$. Then $\mathfrak{p}$ factors in $\mathcal{O}_L$ as

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

where the $\mathfrak{P}_i$ ranger over the primes of $\mathcal{O}_L$ laying over $\mathfrak{p}$.

[1] For the actual statement and a proof of this theorem, see [NS99] Theorem VII.13.4.

idef?

Definition 1.2.6. The prime $\mathfrak{p}$ *ramifies* in L if $e_i > 1$ for some $1 \leq i \leq g$. Otherwise $\mathfrak{p}$ is *unramified*. If also $g = 1$ and $f_1 = 1$, then $\mathfrak{p}$ is *totally ramified*.

Definition 1.2.7. The prime $\mathfrak{p}$ is *inert* in L if $\mathfrak{p}\mathcal{O}_L$ is prime. In this case we have $g = 1$ and $e_1 = 1$.

Definition 1.2.8. The prime $\mathfrak{p}$ *splits* in L if $g > 1$. If also $g = [L : K]$, then $\mathfrak{p}$ *splits completely* or is *totally split*.

Exercise 1.2.9 (See [Mar77, Ch. 4, Exercise 24])**.** Prove the following properties.

(a) If $\mathfrak{p}$ it totally ramified in L then it is totally ramified in K.

(b) Let L' be another extension of K. If $\mathfrak{p}$ is totally ramified in L and unramified in L' then $L \cap L' = K$.

Exercise 1.2.10. Let K be a number field and d_K the discriminant of K Prove that a prime p divides d_K if and only if p ramifies in K.

[*Hint*: This is proved in many books, see for example [Mar77, Thm. 24] or [NS99, Cor. III.2.12]]

1.3 The Decomposition Group

Suppose K is a number field that is Galois over $\mathbb{Q}$ with group $G = \mathrm{Gal}(K/\mathbb{Q})$. Fix a prime $\mathfrak{p} \subset \mathcal{O}_K$ lying over $p \in \mathbb{Z}$.

Definition 1.3.1 (Decomposition group)**.** The *decomposition group* of $\mathfrak{p}$ is the subgroup

$$D_{\mathfrak{p}} = \{\sigma \in G \colon \sigma(\mathfrak{p}) = \mathfrak{p}\} \subset G.$$

Note that $D_{\mathfrak{p}}$ is the stabilizer of $\mathfrak{p}$ for the action of G on the set of primes lying over p.

It also makes sense to define decomposition groups for relative extensions L/K, but for simplicity and to fix ideas in this section we only define decomposition groups for a Galois extension $K/\mathbb{Q}$.

Let $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ denote the residue class field of $\mathfrak{p}$. In this section we will prove that there is an exact sequence

$$1 \to I_{\mathfrak{p}} \to D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p) \to 1,$$

where $I_{\mathfrak{p}}$ is the *inertia subgroup* of $D_{\mathfrak{p}}$, and $\#I_{\mathfrak{p}} = e = e(\mathfrak{p}/p)$. The most interesting part of the proof is showing that the natural map $D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$

is surjective. We will also discuss the structure of $D_{\mathfrak{p}}$ and introduce Frobenius elements, which play a crucial role in understanding Galois representations.

Recall from Theorem 1.2.4 that G acts transitively on the set of primes $\mathfrak{p}$ lying over p. The orbit-stabilizer theorem implies that $[G : D_{\mathfrak{p}}]$ equals the cardinality of the orbit of $\mathfrak{p}$, which by Theorem 1.2.4 equals the number g of primes lying over p, so $[G : D_{\mathfrak{p}}] = g$.

Lemma 1.3.2. *The decomposition subgroups $D_{\mathfrak{p}}$ corresponding to primes $\mathfrak{p}$ lying over a given p are all conjugate as subgroups of G.*

Proof. See Exercise 1.3.3. □

Exercise 1.3.3. Prove Lemma 1.3.2.

[*Hint*: For $\sigma, \tau \in G$ you need to show $\tau D_{\mathfrak{p}} \tau^{-1} = D_{\tau\mathfrak{p}}$. Start by writing down what it means for $\sigma \in D_{\mathfrak{p}}$ and $\tau\sigma\tau^{-1} \in D_{\tau\mathfrak{p}}$.]

The decomposition group is useful because it allows us to refine the extension $K/\mathbb{Q}$ into a tower of extensions, such that at each step in the tower we understand the splitting behavior of the primes lying over p.

Recall the correspondence between subgroups of the Galois group G and subfields of K. The fixed fields corresponding to the decomposition and inertia subgroups have an important description in terms of the splitting behavior of the prime $\mathfrak{p}$. We characterize the fixed field of $D = D_{\mathfrak{p}}$ as follows.

Proposition 1.3.4. *The fixed field*

$$K^D = \{a \in K : \sigma(a) = a \text{ for all } \sigma \in D\}$$

of D is the smallest subfield $F \subset K$ such that there is a unique prime of $\mathcal{O}_K$ lying over $\mathfrak{q} = \mathfrak{p} \cap \mathcal{O}_F$.

Proof. First suppose $F = K^D$, and note that by Galois theory $\mathrm{Gal}(K/F) \cong D$. By Theorem 1.2.4, the group D acts transitively on the primes of K lying over $\mathfrak{q}$. One of these primes is $\mathfrak{p}$, and D fixes $\mathfrak{p}$ by definition, so there is only one prime of K lying over $\mathfrak{q}$. Conversely, if $F \subset K$ is such that $\mathfrak{q}$ lies under a unique prime in K, then $\mathrm{Gal}(K/F)$ fixes $\mathfrak{p}$ (since it is the only prime over $\mathfrak{q}$), so $\mathrm{Gal}(K/F) \subset D$, hence $K^D \subset F$. □

Thus p does not split in going from K^D to K—it does some combination of ramifying and staying inert. To fill in more of the picture, the following proposition asserts that p splits completely and does not ramify in $K^D/\mathbb{Q}$.

Proposition 1.3.5. *Fix a finite Galois extension K of $\mathbb{Q}$, let $\mathfrak{p}$ be a prime lying over p with decomposition group D, and set $F = K^D$ and $\mathfrak{q} = \mathfrak{p} \cap \mathcal{O}_F$. Let g be the number of primes of K lying over p. Then*

$$e(\mathfrak{q}/p) = f(\mathfrak{q}/p) = 1, \quad e(\mathfrak{p}/p) = e(\mathfrak{p}/\mathfrak{q}), \quad f(\mathfrak{p}/p) = f(\mathfrak{p}/\mathfrak{q}), \quad \text{and } g = [F : \mathbb{Q}].$$

Proof. As mentioned right after Definition 1.3.1, the orbit-stabilizer theorem implies that $g = [G : D]$, and by Galois theory $[G : D] = [F : \mathbb{Q}]$, so $g = [F : \mathbb{Q}]$. By Proposition 1.3.4, $\mathfrak{p}$ is the only prime of K lying over $\mathfrak{q}$ so by Theorem 1.2.4,

$$\begin{aligned} e(\mathfrak{p}/\mathfrak{q}) \cdot f(\mathfrak{p}/\mathfrak{q}) = [K : F] &= \frac{[K : \mathbb{Q}]}{[F : \mathbb{Q}]} \\ &= \frac{e(\mathfrak{p}/p) \cdot f(\mathfrak{p}/p) \cdot g}{[F : \mathbb{Q}]} \\ &= e(\mathfrak{p}/p) \cdot f(\mathfrak{p}/p). \end{aligned}$$

Now $e(\mathfrak{p}/\mathfrak{q}) \leq e(\mathfrak{p}/p)$ and $f(\mathfrak{p}/\mathfrak{q}) \leq f(\mathfrak{p}/p)$, so we must have $e(\mathfrak{p}/\mathfrak{q}) = e(\mathfrak{p}/p)$ and $f(\mathfrak{p}/\mathfrak{q}) = f(\mathfrak{p}/p)$. Since from Exercise 1.2.3 we have $e(\mathfrak{p}/p) = e(\mathfrak{p}/\mathfrak{q}) \cdot e(\mathfrak{q}/p)$ and $f(\mathfrak{p}/q) = f(\mathfrak{p}/\mathfrak{q}) \cdot f(\mathfrak{q}/p)$, it follows that $e(\mathfrak{q}/p) = f(\mathfrak{q}/p) = 1$. □

We summarize the results of the decomposition of a prime in the tower $K \supseteq K^D \supseteq \mathbb{Q}$ in Table 1.1. This table shows the ramification indices, inertia degrees, and the number of primes at each step of the tower.

Ramification (e)	Inertia (f)	Splitting (g)	Primes	Fields
			$\mathfrak{p}$	K
$e(\mathfrak{p}/p)$	$f(\mathfrak{p}/p)$	1	|	|
			$\mathfrak{q}$	K^D
1	1	$[K^D : \mathbb{Q}]$	|	|
			p	$\mathbb{Q}$

Table 1.1: Decomposition in the fixed field K^D.

Exercise 1.3.6. Give an example of each of the following:

1. A finite nontrivial Galois extension K of $\mathbb{Q}$ and a prime ideal $\mathfrak{p}$ such that $D_\mathfrak{p} = \mathrm{Gal}(K/\mathbb{Q})$.

2. A finite nontrivial Galois extension K of $\mathbb{Q}$ and a prime ideal $\mathfrak{p}$ such that $D_\mathfrak{p}$ has order 1.

3. A finite Galois extension K of $\mathbb{Q}$ and a prime ideal $\mathfrak{p}$ such that $D_\mathfrak{p}$ is not a normal subgroup of $\mathrm{Gal}(K/\mathbb{Q})$.

4. A finite Galois extension K of $\mathbb{Q}$ and a prime ideal $\mathfrak{p}$ such that $I_\mathfrak{p}$ is not a normal subgroup of $\mathrm{Gal}(K/\mathbb{Q})$.

1.3.1 Galois groups of finite fields

Each $\sigma \in D = D_\mathfrak{p}$ acts in a well-defined way on the finite field $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$, so we obtain a homomorphism

$$\varphi : D_\mathfrak{p} \to \mathrm{Aut}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p).$$

We pause for a moment and review a few basic properties of extensions of finite fields. In particular, they turn out to be Galois so the map φ above is actually a map $D_\mathfrak{p} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$. The properties in this section are general properties of Galois groups for finite fields.

Definition 1.3.7. Let k be any field of characteristic p. Define $\mathrm{Frob}_p : k \to k$ to be the homomorphism given by $a \mapsto a^p$. The map Frob_p is called the *Frobenius* homomorphism.

Exercise 1.3.8.

1. Show the map Frob_p is in fact a field homomorphism, that is $\mathrm{Frob}_p(a+b) = \mathrm{Frob}_p(a) + \mathrm{Frob}_p(b)$ and $\mathrm{Frob}_p(ab) = \mathrm{Frob}_p(a)\,\mathrm{Frob}_p(b)$.

2. Suppose $k = \mathbb{F}_p$. Then show $\mathrm{Frob}_p = id$, i.e., $a^p = a$ for any $a \in \mathbb{F}_p$.

3. Suppose $k = \mathbb{F}_q$ where $q = p^f$ for some $f \geq 1$. Show that $\mathrm{Frob}_p : k \to k$ is an automorphism.

4. Continuing the previous part, note that by Exercise **??**, k^* is cyclic. Let $a \in k$ be a generator for k^*, so a has multiplicative order $p^f - 1$ and $k = \mathbb{F}_p(a)$. Show that

$$\mathrm{Frob}_p^n(a) = a^{p^n} = a \quad \Leftrightarrow \quad (p^f - 1) \mid p^n - 1 \quad \Leftrightarrow \quad f \mid n$$

Remark 1.3.9. Exercise 1.3.8 shows that all finite fields are *perfect*. For more on perfect fields see a standard abstract algebra text such as [DF04].

By Exercise 1.3.8(b,c) the map Frob_p is an automorphism of $\mathbb{F}_\mathfrak{p}$ fixing $\mathbb{F}_p$ and hence defines an element in $\mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$. Let $f = f_{\mathfrak{p}/p}$ be the residue degree of $\mathfrak{p}$, i.e., $f = [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$. Exercise 1.3.8(d) shows the order of Frob_p

is f. Since the order of the automorphism group of a field extension is at most the degree of the extension, we conclude that $\mathrm{Aut}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ is generated by Frob_p. This shows $\mathrm{Aut}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ has order equal to the degree $[\mathbb{F}_\mathfrak{p}/\mathbb{F}_p]$ so we conclude that $\mathbb{F}_\mathfrak{p}/\mathbb{F}_p$ is Galois. We summarize the discussion into the following theorem.

Theorem 1.3.10. *The extension* $\mathbb{F}_\mathfrak{p}/\mathbb{F}_p$ *is Galois and moreover,* $\mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ *is generated by the Frobenius map* Frob_p *defined by* $a \mapsto a^p$.

Exercise 1.3.11. Prove that up to isomorphism there is exactly one finite field of each degree.

[*Hint*: By Theorem 1.3.10 all elements in a finite field satisfy an equation of the form $x^{p^f} - x$ where p is the characteristic and f is the degree over $\mathbb{F}_p$.
]

1.3.2 The Exact Sequence

Because $D_\mathfrak{p}$ preserves $\mathfrak{p}$, there is a natural reduction homomorphism

$$\varphi : D_\mathfrak{p} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p).$$

Theorem 1.3.12. *The homomorphism* φ *is surjective.*

Proof. Let $D = D_\mathfrak{p}$ and $\tilde{a} \in \mathbb{F}_\mathfrak{p}$ be an element such that $\mathbb{F}_\mathfrak{p} = \mathbb{F}_p(\tilde{a})$. Lift $\tilde{a}$ to an algebraic integer $a \in \mathcal{O}_K$, and let $h = \prod_{\sigma \in D}(x - \sigma(a)) \in K^D[x]$. Let $\tilde{h}$ be the reduction of h modulo $\mathfrak{p}$. Note that $h(a) = 0$ so $\tilde{h}(\tilde{a}) = 0$.

Note that the coefficients of h lie in $\mathcal{O}_{K^D}$. By Proposition 1.3.5, the residue field of $\mathcal{O}_{K^D}$ is $\mathbb{F}_p$ so $\tilde{h} \in \mathbb{F}_p[x]$. Therefore $\tilde{h}$ is a multiple of the minimal polynomial of $\tilde{a}$ over $\mathbb{F}_p$. In particular, $\mathrm{Frob}_p(\tilde{a})$ must also be a root of $\tilde{h}$. Since the roots of $\tilde{h}$ are of the form $\widetilde{\sigma(a)}$ this shows that $\widetilde{\sigma(a)} = \mathrm{Frob}_p(\tilde{a})$ for some $\sigma \in D$. Hence $\varphi(\sigma)(\tilde{a}) = \mathrm{Frob}_p(\tilde{a})$. Since elements of $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{F}_p)$ are determined by their action on $\tilde{a}$ by choice of $\tilde{a}$, it follows that $\varphi(\sigma) = \mathrm{Frob}_p$ and hence φ is surjective because Frob_p generates $\mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$. □

Definition 1.3.13 (Inertia Group)**.** The *inertia group associated to* $\mathfrak{p}$ is the kernel $I_\mathfrak{p}$ of the map $D_\mathfrak{p} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$.

We have an exact sequence of groups

$$1 \to I_\mathfrak{p} \to D_\mathfrak{p} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p) \to 1. \tag{1.2}$$

The inertia group is a measure of how p ramifies in K.

Corollary 1.3.14. *We have* $\#I_{\mathfrak{p}} = e = e(\mathfrak{p}/p)$.

Proof. The exact sequence (1.2) implies that $\#I_{\mathfrak{p}} = \#D_{\mathfrak{p}}/f$ where $f = f(\mathfrak{p}/p) = [\mathbb{F}_{\mathfrak{p}} : \mathbb{F}_p]$. Applying Propositions 1.3.4 and 1.3.5, we have

$$\#D_{\mathfrak{p}} = \left[K : K^D\right] = \frac{[K:\mathbb{Q}]}{g} = \frac{efg}{g} = ef.$$

Dividing both sides by f proves the corollary. □

We have the following characterization of $I_{\mathfrak{p}}$.

Proposition 1.3.15. *Let $K/\mathbb{Q}$ be a Galois extension with group G, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ lying over a prime p. Then*

$$I_{\mathfrak{p}} = \{\sigma \in G : \sigma(a) \equiv a \pmod{\mathfrak{p}} \textit{ for all } a \in \mathcal{O}_K\}.$$

Proof. By definition $I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} \colon \sigma(a) \equiv a \pmod{\mathfrak{p}}$ for all $a \in \mathcal{O}_K\}$, so it suffices to show that if $\sigma \notin D_{\mathfrak{p}}$, then there exists $a \in \mathcal{O}_K$ such that $\sigma(a) \not\equiv a \pmod{\mathfrak{p}}$. If $\sigma \notin D_{\mathfrak{p}}$, then $\sigma^{-1} \notin D_{\mathfrak{p}}$, so $\sigma^{-1}(\mathfrak{p}) \neq \mathfrak{p}$. Since both are maximal ideals, there exists $a \in \mathfrak{p}$ with $a \notin \sigma^{-1}(\mathfrak{p})$, i.e., $\sigma(a) \notin \mathfrak{p}$. Thus $\sigma(a) \not\equiv a \pmod{\mathfrak{p}}$. □

Exercise 1.3.16. Let $I = I_{\mathfrak{p}}$ be the inertia subgroup as above. Show that

1. K^I is the largest subfield of K such that p is unramified in K^I.

2. K^I is the smallest subfield of K such that $\mathfrak{p}$ is totally ramified over $\mathfrak{p} \cap K^I$.

Figure 1.1 summarizes the relationship between I, D, and the splitting of p in K. The dots on the left represent primes lying over p. The size of the dot represents the inertia degree. Compare this with Table 1.1.

1.4 Frobenius Elements

Suppose that $K/\mathbb{Q}$ is a finite Galois extension with group G and p is a prime such that $e = 1$ (i.e., an unramified prime). Then $I = I_{\mathfrak{p}} = 1$ for any $\mathfrak{p} \mid p$, so the map φ of Theorem 1.3.12 is a canonical isomorphism $D_{\mathfrak{p}} \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}, \mathbb{F}_p)$. By Section 1.3.1, the group $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}, \mathbb{F}_p)$ is cyclic with canonical generator Frob_p. The *Frobenius element* corresponding to $\mathfrak{p}$ is $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$. It is the unique (see Exercise 1.4.1) element of G such that for all $a \in \mathcal{O}_K$ we have

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

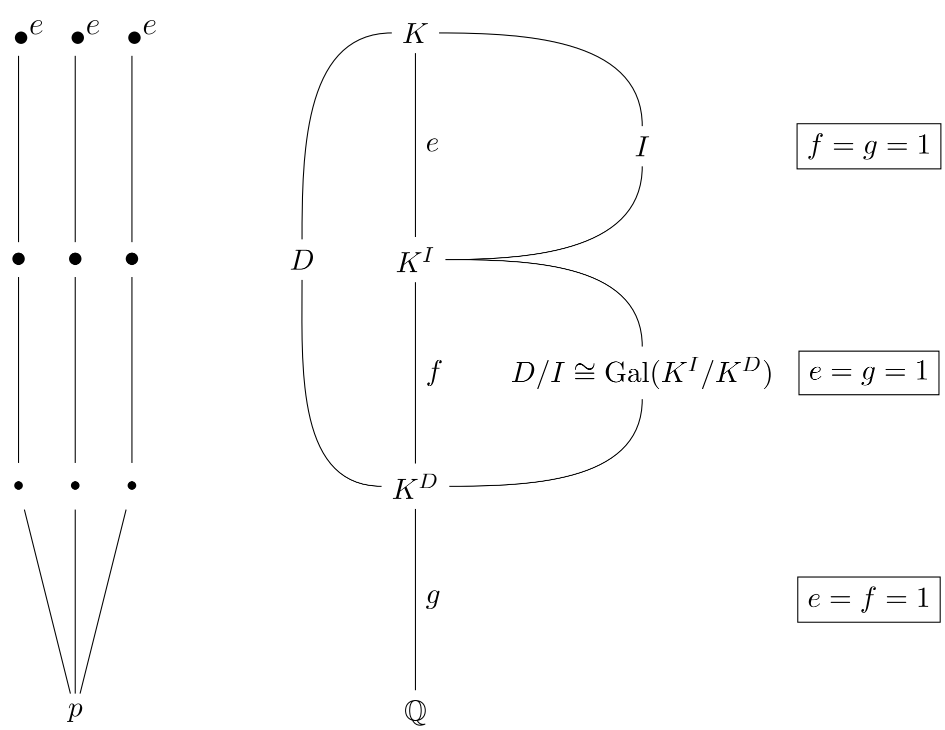

Figure 1.1: Splitting of p in a Galois extension $K/\mathbb{Q}$.

Exercise 1.4.1. With the notation above, prove that $\mathrm{Frob}_\mathfrak{p}$ is unique. That is, if σ satisfies $\sigma(a) \equiv a^p \pmod{\mathfrak{p}}$ for all $a \in \mathcal{O}_K$ then $\sigma = \mathrm{Frob}_\mathfrak{p}$.

[*Hint*: First show $\sigma \in D_\mathfrak{p}$, then argue as in the proof of Proposition 1.3.15.]

Just as the primes $\mathfrak{p}$ and decomposition groups $D_\mathfrak{p}$ are all conjugate, the Frobenius elements corresponding to primes $\mathfrak{p} \mid p$ are all conjugate as elements of G.

Proposition 1.4.2. *For each $\sigma \in G$, we have*

$$\mathrm{Frob}_{\sigma\mathfrak{p}} = \sigma \,\mathrm{Frob}_\mathfrak{p}\, \sigma^{-1}.$$

In particular, the Frobenius elements lying over a given prime are all conjugate.

Proof. Fix $\sigma \in G$. For any $a \in \mathcal{O}_K$ we have $\mathrm{Frob}_\mathfrak{p}(\sigma^{-1}(a)) - \sigma^{-1}(a)^p \in \mathfrak{p}$. Applying σ to both sides, we see that $\sigma \,\mathrm{Frob}_\mathfrak{p}(\sigma^{-1}(a)) - a^p \in \sigma\mathfrak{p}$, so $\sigma \,\mathrm{Frob}_\mathfrak{p}\, \sigma^{-1} = \mathrm{Frob}_{\sigma\mathfrak{p}}$. □

Thus the conjugacy class of $\mathrm{Frob}_\mathfrak{p}$ in G is a well-defined function of p. For example, if G is abelian, then $\mathrm{Frob}_\mathfrak{p}$ does not depend on the choice of $\mathfrak{p}$ lying over p and we obtain a well defined symbol $\left(\frac{K/\mathbb{Q}}{p}\right) = \mathrm{Frob}_\mathfrak{p} \in G$ called the *Artin symbol*. It extends to a homomorphism from the free abelian group on unramified primes p to G. Class field theory (for $\mathbb{Q}$) sets up a natural bijection between abelian Galois extensions of $\mathbb{Q}$ and certain maps from certain subgroups of the group of fractional ideals for $\mathbb{Z}$ (i.e., $\mathbb{Q}^*$). We have just described one direction of this bijection, which associates to an abelian extension the Artin symbol (which is a homomorphism).

The Kronecker-Weber theorem asserts that the abelian extensions of $\mathbb{Q}$ are exactly the subfields of the fields $\mathbb{Q}(\zeta_n)$, as n varies over all positive integers. By Galois theory there is a correspondence between the subfields of the field $\mathbb{Q}(\zeta_n)$, which has Galois group $(\mathbb{Z}/n\mathbb{Z})^*$, and the subgroups of $(\mathbb{Z}/n\mathbb{Z})^*$. If $H \subseteq (\mathbb{Z}/n\mathbb{Z})^*$ is the subgroup corresponding to $K \subset \mathbb{Q}(\zeta_n)$ then the Artin reciprocity map $p \mapsto \left(\frac{K/\mathbb{Q}}{p}\right)$ is given by $p \mapsto [p] \in (\mathbb{Z}/n\mathbb{Z})^*/H$.

Remark 1.4.3. Notice above that the n used is not unique. That is, if K is an abelian extension of $\mathbb{Q}$ then it lies in some $\mathbb{Q}(\zeta_n)$. But then it also lies inside of $\mathbb{Q}(\zeta_{dn})$ for any positive integer d. However, a different choice of n would mean a different choice of H. However the quotient $(\mathbb{Z}/n\mathbb{Z})^*/H$ used is not dependent on n since it is isomorphic to the Galois group of $K/\mathbb{Q}$.

1.5 The Artin Conjecture

The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is an object of central importance in number theory, and we can interpret much of number theory as the study of this group. A good way to study a group is to study how it acts on various objects, that is, to study its representations.

Endow $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with the topology which has as a basis of open neighborhoods of the origin the subgroups $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, where K varies over finite Galois extensions of $\mathbb{Q}$. Fix a positive integer n and let $\mathrm{GL}_n(\mathbb{C})$ be the group of $n \times n$ invertible matrices over $\mathbb{C}$ with the discrete topology.

Warning 1.5.1. The topology on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is **not** the topology induced by taking as a basis of open neighborhoods around the origin the collection of finite-index normal subgroups of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, see [Mil14, Ch. 7] or Exercise 1.5.5. In particular, there exist nonopen normal subgroups of finite index which do not correspond to subgroups $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for some finite Galois extension $K/\mathbb{Q}$.

Definition 1.5.2. A *complex n-dimensional representation* of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a continuous homomorphism

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C}).$$

For ρ to be continuous means that if K is the fixed field of $\ker(\rho)$, then $K/\mathbb{Q}$ is a finite Galois extension. We have a diagram

$$\begin{tikzcd}
\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[rr, "\rho"] \arrow[dr] & & \mathrm{GL}_n(\mathbb{C}) \\
& \mathrm{Gal}(K/\mathbb{Q}) \arrow[ur, hook, "\rho'"'] &
\end{tikzcd}$$

Exercise 1.5.3. Suppose $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ is continuous. Show that the image is finite.

Remark 1.5.4. The converse to Exercise 1.5.3 is **false** in general (see Exercise 1.5.5). This is essentially the same warning as Warning 1.5.1, however it is worth pointing out to avoid mistakes.[2]

Exercise 1.5.5. Find a nonopen subgroup of index 2 in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Note this is also an example of a non-continuous homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ with finite image.

[2] See [Kim94, pg. 1].

[*Hint*: Use Zorn's lemma to show that there are homomorphisms $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$ with finite image that are not continuous, since they do not factor through the Galois group of any finite Galois extension.]

Exercise 1.5.6. Let S_3 by the symmetric group on three symbols, which has order 6.

1. Observe that $S_3 \cong D_3$, where D_3 is the dihedral group of order 6, which is the group of symmetries of an equilateral triangle.

2. Use (1) to write down an explicit embedding $S_3 \hookrightarrow \mathrm{GL}_2(\mathbb{C})$.

3. Let K be the number field $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega^3 = 1$ is a nontrivial cube root of unity. Show that K is a Galois extension with Galois group isomorphic to S_3.

4. We thus obtain a 2-dimensional irreducible complex Galois representation
$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \cong S_3 \subset \mathrm{GL}_2(\mathbb{C}).$$
Compute a representative matrix of Frob_p and the characteristic polynomial of Frob_p for $p = 5, 7, 11, 13$.

Fix a Galois representation ρ and let K be the fixed field of $\ker(\rho)$, so ρ factors through $\mathrm{Gal}(K/\mathbb{Q})$. For each prime $p \in \mathbb{Z}$ that is not ramified in K, there is an element $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(K/\mathbb{Q})$ that is well-defined up to conjugation by elements of $\mathrm{Gal}(K/\mathbb{Q})$. This means that $\rho'(\mathrm{Frob}_p) \in \mathrm{GL}_n(\mathbb{C})$ is well-defined up to conjugation. Thus the characteristic polynomial $F_p(x) \in \mathbb{C}[x]$ of $\rho'(\mathrm{Frob}_p)$ is a well-defined invariant of p and ρ. Let

$$R_p(x) = x^{\deg(F_p)} \cdot F_p(1/x) = 1 + \cdots + \det(\mathrm{Frob}_p) \cdot x^{\deg(F_p)}$$

be the polynomial obtain by reversing the order of the coefficients of F_p. Following E. Artin [Art23, Art30], set

$$L(\rho, s) = \prod_{p \text{ unramified}} \frac{1}{R_p(p^{-s})}. \tag{1.3}$$

We view $L(\rho, s)$ as a function of a single complex variable s. One can prove that $L(\rho, s)$ is holomorphic on some right half plane, and extends to a meromorphic function on all $\mathbb{C}$.

Conjecture 1.5.7 (Artin). *The L-function of any continuous representation*

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$$

is an entire function on all $\mathbb{C}$, except possibly at 1.

This conjecture asserts that there is some way to analytically continue $L(\rho, s)$ to the whole complex plane, except possibly at 1. (A standard fact from complex analysis is that this analytic continuation must be unique.) The simple pole at $s = 1$ corresponds to the trivial representation (the Riemann zeta function), and if $n \geq 2$ and ρ is irreducible, then the conjecture is that ρ extends to a holomorphic function on all $\mathbb{C}$.

The conjecture is known when $n = 1$. Assume for the rest of this paragraph that ρ is odd, i.e., if $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is complex conjugation, then $\det(\rho(c)) = -1$. When $n = 2$ and the image of ρ in $\mathrm{PGL}_2(\mathbb{C})$ is a solvable group, the conjecture is known, and is a deep theorem of Langlands and others (see [Lan80]), which played a crucial roll in Wiles's proof of Fermat's Last Theorem. When $n = 2$ and the image of ρ in $\mathrm{PGL}_2(\mathbb{C})$ is not solvable, the only possibility is that the projective image is isomorphic to the alternating group A_5. Because A_5 is the symmetry group of the icosahedron, these representations are called *icosahedral*. In this case, Joe Buhler's Harvard Ph.D. thesis [Buh78] gave the first example in which ρ was shown to satisfy Conjecture 1.5.7. There is a book [Fre94], which proves Artin's conjecture for 7 icosahedral representation (none of which are twists of each other). Kevin Buzzard and the author proved the conjecture for 8 more examples [BS02]. Subsequently, Richard Taylor, Kevin Buzzard, Nick Shepherd-Barron, and Mark Dickinson proved the conjecture for an infinite class of icosahedral Galois representations (disjoint from the examples) [BDSBT01]. The general problem for $n = 2$ is in fact now completely solved, due to recent work of Khare and Wintenberger [KW08] that proves Serre's conjecture.

Bibliography

[Art23] E. Artin, *Über eine neue Art von L-reihen*, Abh. Math. Sem. Univ. Hamburg **3** (1923), 89–108.

[Art30] E Artin, *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren*, Abh. math. Semin. Univ. Hamburg **8** (1930), 292–306.

[BDSBT01] Kevin Buzzard, Mark Dickinson, Nick Shepherd-Barron, and Richard Taylor, *On icosahedral Artin representations*, Duke Math. J. **109** (2001), no. 2, 283–318. MR 1845181 (2002k:11078)

[BS02] K. Buzzard and W. A. Stein, *A mod five approach to modularity of icosahedral Galois representations*, Pacific J. Math. **203** (2002), no. 2, 265–282. MR 2003c:11052

[Buh78] J. P. Buhler, *Icosahedral Galois representations*, Springer-Verlag, Berlin, 1978, Lecture Notes in Mathematics, Vol. 654.

[DF04] D.S. Dummit and R.M. Foote, *Abstract Algebra*, Wiley, 2004.

[Fre94] G. Frey (ed.), *On Artin's conjecture for odd 2-dimensional representations*, Springer-Verlag, Berlin, 1994, 1585. MR 95i:11001

[Kim94] Ian Kiming, *On the experimental verification of the artin conjecture for 2-dimensional odd galois representations over q liftings of 2-dimensional projective galois representations over q*, On Artin's Conjecture for Odd 2-dimensional Representations (Gerhard Frey, ed.), Lecture Notes in Mathematics, vol. 1585, Springer Berlin Heidelberg, 1994, pp. 1–36 (English).

[KW08] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (i)*, Preprint (2008).

[Lan80] R. P. Langlands, *Base change for* GL(2), Princeton University Press, Princeton, N.J., 1980.

[Mar77] Daniel A. Marcus, *Number Fields*, Universitext (1979), Springer, 1977.

[Mil14] James S. Milne, *Fields and Galois Theory (v4.50)*, 2014, Available at `http://www.jmilne.org/math/`, p. 138.

[NS99] J. Neükirch and N. Schappacher, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, Springer Berlin Heidelberg, 1999.