The Chebotarev Density Theorem and Applications to Computing Galois Groups

Alejandro De Las Peñas Castaño

02/december/2021

1 Notation and Preliminaries

The following notation will be fixed:

- K is a number field, i.e. a finite extension of $\mathbb{Q}$.
- L is a finite Galois extension of K, of degree n and Galois group $G := \text{Gal}(L/K)$.
- $\mathcal{O}_K$ and $\mathcal{O}_L$ will denote the ring of integers of K and L respectively.
- $\mathfrak{p} \subset \mathcal{O}_K$ is a nonzero prime ideal and $\mathfrak{P} \subset \mathcal{O}_L$ is a nonzero prime lying over $\mathfrak{p}$, that is $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.
- $k := \mathcal{O}_K/\mathfrak{p}$ and $\ell := \mathcal{O}_L/\mathfrak{P}$ are the residue fields of $\mathfrak{p}$ and $\mathfrak{P}$ respectively. In particular, k is a finite field and we denote its size by q, so $q = p^\nu$ for some $\nu \geq 1$ and $p \in \mathbb{Z}$ the prime number such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Furthermore, ℓ/k is a finite extension of finite fields and is thus a Galois extension.
- (Fundamental Identity) Since L/K is Galois, then the (unique) factorization of the extension $\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_L$ is of the form

  $$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e \cdots \mathfrak{P}_g^e$$

  where $\mathfrak{P}_1, \ldots, \mathfrak{P}_g \subset \mathcal{O}_L$ are nonzero prime ideals and

  $$n = efg$$

  where

  $$f = [\mathcal{O}_L/\mathfrak{P}_1 : \mathcal{O}_K/\mathfrak{p}] = \cdots = [\mathcal{O}_L/\mathfrak{P}_g : \mathcal{O}_K/\mathfrak{p}]$$

  is the inertia degree and e is the ramification index.

Next we go over the basic facts and definitions required to state and use the Chebotarev Density Theorem.

Theorem 1.1. *Let $\{\mathfrak{P}_1 \ldots, \mathfrak{P}_g\}$ be the set of prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Then the Galois group G acts transitively on this set via:*

$$G \curvearrowright \{\mathfrak{P}_1 \ldots, \mathfrak{P}_g\} \quad \textit{with} \quad \sigma\mathfrak{P}_i = \{\sigma(x) \mid x \in \mathfrak{P}_i\}.$$

Definition. The *decomposition group* of $\mathfrak{P}$ over $\mathfrak{p}$ is the stabilizer of $\mathfrak{P}$ under the action defined in Theorem 1.1. More precisely:

$$D(\mathfrak{P}) := D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$$

Remarks 1.2. (about the Decomposition Group)

(1.2.1) If $\sigma \in G$, then

$$D(\sigma\mathfrak{P}) = \sigma D(\mathfrak{P})\sigma^{-1}.$$

This is a general phenomenon that occurs when conjugating stabilizers of elements under group actions.

(1.2.2) By the Orbit-Stabilizer Theorem,[1] the number of distinct primes lying above $\mathfrak{p}$ is equal to the index of the decomposition group. More precisely

$$\big[G : D(\mathfrak{P})\big] = g. \tag{1}$$

Plugging this into the fundamental identity, we get

$$efg = n = |G| = |D(\mathfrak{P})| \cdot [G : D(G)] = |D(G)|g \quad \Longrightarrow \quad |D(G)| = ef. \tag{2}$$

(1.2.3) By (1), we conclude that

$$D(\mathfrak{P}) = \{1\} \quad \Longleftrightarrow \quad \mathfrak{p} \text{ splits completely.}$$

Intuitively speaking, the smaller $D(\mathfrak{P})$ is, the more primes $\mathfrak{p}$ splits into inside L.

(1.2.4) Similarly, we have

$$D(\mathfrak{P}) = G \quad \Longleftrightarrow \quad \mathfrak{p} \text{ is nonsplit} \quad \Longleftrightarrow \quad \mathfrak{p}\mathcal{O}_L = \mathfrak{P}^e.$$

This case includes the case when $\mathfrak{p}$ is totally ramified or when $\mathfrak{p}$ is inert.

(1.2.5) If $\sigma \in D(\mathfrak{P})$, then by definition σ descends to an automorphism

$$\overline{\sigma} : \ell \longrightarrow \ell \quad \text{defined as} \quad \overline{\sigma}(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}.$$

Then, the *restriction map*

$$\text{res} : D(\mathfrak{P}) \longrightarrow \text{Gal}(\ell/k) \quad \text{defined by} \quad \sigma \mapsto \overline{\sigma}$$

is a surjective group homomorphism.[2]

Definition. The *inertia group* of $\mathfrak{P}$ over $\mathfrak{p}$, denoted by $I(\mathfrak{P})$ is the kernel of the restriction map defined in (1.2.5). More explicitly,

$$I(\mathfrak{P}) := \{\sigma \in D(\mathfrak{P}) \mid \sigma(x) \equiv x \,(\text{mod } \mathfrak{P}) \ \ \forall x \in \mathcal{O}_L\}$$

Remarks 1.3. (about the inertia group)

(1.3.1) Since the restriction map is surjective, it factors through the quotient $D(\mathfrak{P})/I(\mathfrak{P})$ as an isomprhism onto $\text{Gal}(\ell/k)$. In particular:

$$\big[D(\mathfrak{P}) : I(\mathfrak{P})\big] = f.$$

Plugging this into (2) yields

$$|I(\mathfrak{P})| = e.$$

(1.3.2) A trivial but useful consequence of the above, is:

$$I(\mathfrak{P}) = \{1\} \quad \Longleftrightarrow \quad \mathfrak{p} \text{ is unramified.}$$

In words, the inertia group of $\mathfrak{P}$ over $\mathfrak{p}$ measures the ramification of $\mathfrak{p}$ in L.

(1.3.3) By definition of the inertia group, we have the following short exact sequence:

$$1 \longrightarrow I(\mathfrak{P}) \hookrightarrow D(\mathfrak{P}) \xrightarrow{\text{res}} \text{Gal}(\ell/k) \longrightarrow 1$$

[1] See Proposition 2 of §4.1 of [DF04].

[2] See Proposition 9.4 of Chapter 1 of [Neu99]

2 Frobenius Elements

We know that ℓ/k is a finite extension of finite fields and hence Galois. In fact, the extension is cyclic, that is

$$\mathrm{Gal}(\ell/k) = \langle \varphi_q \rangle$$

where $q = |k|$ and φ_q is the *Frobenius automorphism* defined by $\varphi_q(x) = x^q$. Now, if $\mathfrak{p}$ is unramified, then the restriction map is an isomorphism and thus there is a unique element of $D(\mathfrak{P})$ that maps to φ_q. This element, is very important.

Definition. Suppose $\mathfrak{p}$ is unramified and let $\mathfrak{P}$ be a prime lying over $\mathfrak{p}$. The *Frobenius element* of $\mathfrak{P} \mid \mathfrak{p}$, denoted by $(\mathfrak{P}, L/K)$, is the unique element of $D(\mathfrak{P})$ that restricts to the Frobenius automorphism φ_q, that is

$$(\mathfrak{P}, L/K) := \mathrm{res}^{-1}(\varphi_q).$$

More precisely, $\sigma = (\mathfrak{P}, L/K)$ is the unique element of $D(\mathfrak{P})$ that satisfies:

$$\forall x \in \mathcal{O}_L, \quad \sigma(x) \equiv x^q \,(\mathrm{mod}\ \mathfrak{P})$$

Remarks 2.1. (about Frobenius elements)

(2.1.1) Similarly to (1.2.1), we have

$$(\tau\mathfrak{P}, L/K) = \tau(\mathfrak{P}, L/K)\tau^{-1} \qquad (\tau \in G).$$

Therefore, since G acts transitively over the set of primes lying above $\mathfrak{p}$ (see Theorem 1.1), then the conjugacy class of $\sigma := (\mathfrak{P}, L/K)$ is:

$$\{\tau\sigma\tau^{-1} \mid \tau \in G\} = \{(\tau P, L/k) \mid \tau \in G\} = \{(\mathfrak{P}_i, L/K) \mid i = 1, \ldots, g\}.$$

(2.1.2) In view of the above remark, we can slighlty generalize the definition of the Frobenius element as:

$$(\mathfrak{p}, L/K) := \{(\mathfrak{P}_i, L/K) \mid i = 1, \ldots, g\}.$$

We make the standard abuse of notation and write $(\mathfrak{p}, L/K) = (\mathfrak{P}, L/K)$ for some $\mathfrak{P} \mid \mathfrak{p}$ whenever $(\mathfrak{P}, L/K) \in Z(G)$ and thus its conjugacy class is trivial.

(2.1.3) Since $\mathfrak{p}$ is unramified in L/K, then $D(\mathfrak{P}) \cong \mathrm{Gal}(\ell/k)$ and thus $D(\mathfrak{P})$ is cyclic and generated by the Frobenius element, i.e.

$$D(\mathfrak{P}) = \big\langle (\mathfrak{P}, L/K) \big\rangle.$$

(2.1.4) A trivial but important consequence of the above remark and (1.2.3) is that:

$$\mathfrak{p} \text{ splits completely} \quad \Longleftrightarrow \quad (\mathfrak{P}, L/K) = 1 \quad \text{for some } \mathfrak{P} \mid \mathfrak{p}.$$

Examples 2.2. (of Frobenius elements)

(2.2.1) (Quadratic Case) Let $L = \mathbb{Q}(\sqrt{d})$ and $K = \mathbb{Q}$. Observe that the extension is Galois with Galois group $G \cong \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z}$ and in particular it is an abelian extension. The discriminant is d (resp. $4d$) if $d \equiv 1 \,(\mathrm{mod}\ 4)$ (resp. $d \not\equiv 1 \,(\mathrm{mod}\ 4)$). So let $p \in \mathbb{Z}$ be an odd prime such that $p \nmid d$. Then $\mathfrak{p} := p\mathbb{Z}$ is unramified in $\mathbb{Q}(\sqrt{d})$ and $\sigma := (\mathfrak{p}, \mathbb{Q}(\sqrt{d})/\mathbb{Q})$ is a well-defined element of G. By (2.1.4), we have

$$\sigma = 1 \quad \Longleftrightarrow \quad \mathfrak{p} \text{ splits completely in } \mathbb{Q}(\sqrt{d}) \quad \Longleftrightarrow \quad d \text{ is a square in } (\mathbb{Z}/p\mathbb{Z})^\times.$$

Since being a square in $(\mathbb{Z}/p\mathbb{Z})^\times$ is characterized by the Legendre symbol, we conclude that

$$\big(p\mathbb{Z}, \mathbb{Q}(\sqrt{d})/\mathbb{Q}\big) = \left(\frac{d}{p}\right)$$

(2.2.2) (Cyclotomic Case) Let $L = \mathbb{Q}(\zeta)$ where ζ is a primitive mth root of unity, and $K = \mathbb{Q}$. Then a prime number $p \in \mathbb{Z}$ ramifies in $\mathbb{Q}(\zeta)$ if and only if $p \mid m$ (cf. Corollary 10.4 of §1 of [Neu99]), so we may assume that $p \nmid m$. We also know that $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$ via the isomorphism

$$\tau \mapsto j \quad \text{where} \quad \tau(\zeta) = \zeta^j.$$

In particular $\mathbb{Q}(\zeta)$ is abelian and thus $\sigma := (p\mathbb{Z}, \mathbb{Q}(\zeta)/\mathbb{Q})$ is a well-defined element of G. In fact, the Frobenius element σ is defined as $\sigma(\zeta) = \zeta^p$.

Indeed, let $\mathfrak{P}$ be a prime of $\mathbb{Q}(\zeta)$ lying over $p\mathbb{Z}$, and $x \in \mathcal{O}_L = \mathbb{Z}[\zeta]$ written in terms of the integral basis as $x = \sum a_j \zeta^j$ where $a_j \in \mathbb{Z}$. Then:

$$\sigma(x) = \sum a_j \sigma(\zeta)^j = \sum a_j \zeta^{pj} \equiv \sum a_j^p \zeta_j^{jp} \equiv \left(a_j \zeta^j\right)^p = x^p \,(\mathrm{mod}\ p\mathbb{Z}[\zeta])$$

and thus $\sigma(x) \equiv x \,(\mathrm{mod}\ \mathfrak{P})$ as required. This also proves that $\sigma \in D(\mathfrak{P})$ since $\mathfrak{P}$ is a prime ideal. Note that viewed as an element of $(\mathbb{Z}/n\mathbb{Z})^\times$, the Frobenius element is just p mod n.

Remark 2.3. Example (2.2.2) implies the quadratic reciprocity law, see Example 8.18 and its applications in [Mil17].

3 Computing Galois Groups

Identifying Frobenius elements and their cycle types (viewed as permutations of the roots of some polynomial) can help us determine the Galois group of the splitting field of some polynomial. The set up is the following:

- $F \in \mathcal{O}_K[x]$ is a monic polynomial of degree N.
- There is a reduction homomorphism $\mathcal{O}_K[x] \to k[x]$ which we write as $F \mapsto \overline{F}$, where $\overline{F} \in k[x]$ is the polynomial whose coefficients are the reduction mod $\mathfrak{p}$ of the coefficients of F.
- L/K is the splitting field of F with Galois group G.
- If $\{\alpha_1, \ldots, \alpha_N\}$ are the roots of F in L, we identify G with a subgroup of the permutation group S_N acting by permutations on the set of roots.

Then we have the following useful result:

Theorem 3.1. *(Dedekind) Let $F(x) \in \mathcal{O}_K[x]$ be monic and let L be the splitting field of F over K. Suppose that $\overline{F} \in k[x]$ is square-free and factors as a (linear) product of irreducibles in $k[x]$ as*

$$\overline{F} = \overline{F_1} \cdots \overline{F_r}, \qquad (N_i := \deg F_i)$$

Then for any prime ideal $\mathfrak{P}$ of L lying over $\mathfrak{p}$, the Frobenius element $\sigma = (\mathfrak{P}, L/K)$ is a disjoint product of r cycles of lengths $N_1, \ldots, N_r$.

Remarks 3.2. (about Dedekind's Theorem)

(3.2.1) The assumptions on the factorization $\overline{F} = \overline{F_1} \cdots \overline{F_r}$ imply that $\mathfrak{p}$ is unramified in L since $\overline{F}$ is square-free in $(\mathcal{O}_K/\mathfrak{p})[x]$; $\mathfrak{p}$ cannot ramify as this would introduce a square term in the factorization.[3] This implies that the Frobenius element σ is well-defined.

(3.2.2) Dedekind's Theorem says that you can read the cycle type of $(\mathfrak{P}, L/K)$ off of the factorization of F modulo $\mathfrak{P} \cap \mathcal{O}_K$.

Proof. Let $\sigma = (\mathfrak{P}, L/K)$ be a Frobenius element. The choice of prime $\mathfrak{P}$ lying over $\mathfrak{p}$ does not affect the conclusion of the theorem since any two choices are conjugate by (2.1.1) and conjugate permutations have the same cycle structure.

Recall that $\varphi_q = \mathrm{res}(\sigma) = \overline{\sigma}$ is the Frobenius automorphism in $\overline{G} := \mathrm{Gal}(\ell/k)$ and thus acts on the set of roots $\{\beta_1, \ldots, \beta_N\} \subset \ell$ via permutations. Now, write $\overline{F}(x) = (x - \beta_1) \cdots (x - \beta_N)$ and, for any subset of roots $\Omega \subseteq \{\beta_1, \ldots, \beta_N\}$, define

$$\overline{F_\Omega}(x) := \prod_{\beta \in \Omega} (x - \beta).$$

Furthermore, $\overline{F_\Omega}$ is fixed under the action of $\overline{G}$:

$$\varphi_q \overline{F_\Omega} := \prod_{\beta \in \Omega} (x - \varphi_q(\alpha)) = \prod_{\beta \in \varphi_q \Omega} (x - \beta)$$

if and only if $\Omega = \varphi_q \Omega$, i.e. Ω is stable under the action of $\overline{G}$. If $\overline{F_\Omega}$ is fixed under the action of $\overline{G}$, then its coefficients are in k and thus the divisibility condition $\overline{F_\Omega} \mid \overline{F}$ happens in $k[x]$. Since $\Omega' \subseteq \Omega$ implies that $\overline{F_{\Omega'}} \mid \overline{F_\Omega}$, then $\overline{F_\Omega}$ is an irreducible factor of $\overline{F}$ if and only if, Ω is minimal among stable subsets of $\{\beta_1, \ldots, \beta_N\}$, i.e. an orbit of the action. Thus, if there are r' orbits, the ith orbit of length N_i', then:

$$\overline{F} = \overline{F_{\Omega_1}} \cdots \overline{F_{\Omega_{r'}}}$$

where each F_{Ω_i} is irreducible of degree N_i'. By uniqueness of factorization in $k[x]$, we must have $r = r'$ and $N_i = N_i'$.

From elementary group theory, we know that partition of $\{\beta_1, \ldots, \beta_N\}$ into orbits corresponds exactly with the cycle decomposition of φ_q in $\overline{G}$. Finally, since $\overline{G} \cong D(\mathfrak{P})$ (since $\mathfrak{p}$ is unramified), we have that σ has the same cycle structure as φ_q. □

Examples 3.3. (of Dedekind's Theorem)

[3] This is easily verified trivially true if $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some root α and F irreducible, because under these assumptions we have

$$\frac{\mathcal{O}_L}{\mathfrak{p}\mathcal{O}_L} \cong \frac{\mathcal{O}_K[x]/(F)}{\mathfrak{p}\mathcal{O}_K[x]/(F)} \cong \frac{k[x]}{(\overline{F})} \cong \frac{k[x]}{(\overline{F_1})} \times \cdots \times \frac{k[x]}{(\overline{F_r})}$$

where each factor on the RHS is a field. Thus the prime factorization of $\mathfrak{p}\mathcal{O}_L$ is

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{p} + F_1(\alpha)) \cdots (\mathfrak{p} + F_r(\alpha)).$$

and $\mathfrak{p}$ is thus unramified.

(3.3.1) Let $K = \mathbb{Q}$ and consider $F(x) = x^4 + x - 1$. We factor F modulo the following primes:

$$F(x) \equiv \begin{cases} x^4 + x - 1 & \pmod 2 \\ x^4 + x - 1 & \pmod 3 \\ x^4 + x - 1 & \pmod 5 \\ (x+3)(x^3 + 4x^2 + 2x + 2) & \pmod 7 \\ (x+3)(x^3 + 8x^2 + 9x + 7) & \pmod{11} \\ (x+2)(x^3 + 11x^2 + 4x + 6) & \pmod{13} \\ (x+12)(x+15)(x^2 + 7x + 5) & \pmod{17} \\ x^4 + x - 1 & \pmod{19} \\ \quad \vdots & \\ (x^2 + 15x + 32)(x^2 + 56x + 51) & \pmod{71} \\ \quad \vdots & \end{cases}$$

Therefore, if $\mathfrak{P}_p$ is a prime lying over $p\mathbb{Z}$, then the cylce type of $\sigma_p := (\mathfrak{P}_p, L/K)$ is:

$$\sigma_2 = (****), \quad \sigma_7 = (***), \quad \sigma_{17} = (**), \quad \sigma_{71} = (**)(**)$$

Thus we have that the Galois group $G \subseteq S_4$ contains a 4-cycle, a 3-cycle and a transposition. This implies that $G = S_4$.

(3.3.2) Let $K = \mathbb{Q}$ and consider $F(x) = x^5 - x - 1$. We factor F modulo the following primes:

$$F(x) \equiv \begin{cases} (x^2 + x + 1)(x^3 + x^2 + 1) & \pmod 2 \\ x^5 - x - 1 & \pmod 3 \\ x^5 - x - 1 & \pmod 5 \\ (x^2 + 6x + 3)(x^3 + x^2 + 5x + 2) & \pmod 7 \\ x^5 - x - 1 & \pmod{11} \\ x^5 - x - 1 & \pmod{13} \\ (x+9)(x+11)(x^3 + 14x^2 + 12x + 6) & \pmod{17} \\ \cancel{(x+6)^2(x^3 + 7x^2 + 13x + 10)} & \pmod{19} \\ (x+9)(x^4 + 14x^3 + 12x^2 + 7x + 5) & \pmod{23} \\ (x+27)(x^4 + 2x^3 + 4x^2 + 8x + 15) & \pmod{24} \\ \quad \vdots & \\ (x+53)(x^2 + 31x + 65)(x^2 + 50x + 55) & \pmod{67} \\ \quad \vdots & \end{cases}$$

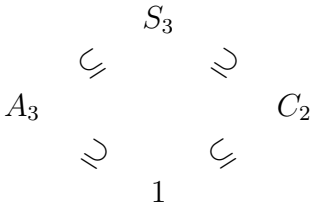
Therefore, if $\mathfrak{P}_p$ is a prime lying over $p\mathbb{Z}$, then the cylce type of $\sigma_p := (\mathfrak{P}_p, L/K)$ is:

$$\sigma_2 = (**)(***), \quad \sigma_3 = (*****), \quad \sigma_{17} = (***), \quad \sigma_{23} = (****), \quad \sigma_{67} = (**)(**)$$

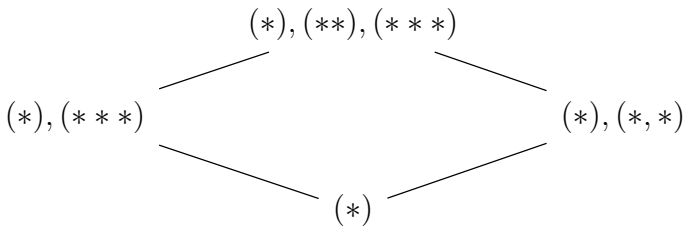
Observe that σ_2^3 is a transposition. Thus we have that the Galois group $G \subseteq S_5$ contains a 5-cycle, a 4-cycle and a transposition. This implies that $G = S_5$.

In these examples we are fortunate to get enough cycle types in our Galois group to be able to conclude that G must be the full permutation group. However, we don't have a guarantee (at least not yet) that any given cycle type will appear, so this ad hoc method may not always give us an answer for the Galois group. To illustrate this, consider the case of cubic polynomials.

The Galois group of a cubic polynomial is a subgroup of S_3 of which there are only four:



whose elements have cycle types:



Thus, if F is a cubic, and we find two primes p_1, p_2 where $F \pmod{p_1}$ is irreducible, and $F \pmod{p_2}$ factors into a quadratic and linear factor, then the Galois group must be S_3 as S_3 is the only subgroup that has both $(**)$ and $(***)$ as possible cycle types.

However, if every time we factor F modulo p we never get a factorization of the type $F(x) \equiv (x+a)(x^2+bx+c) \pmod{p}$, then we should *expect* the Galois group to be A_3. For example, consider the polynomial

$$F(x) = x^3 - 3x - 1$$

Then we have:

$$F(x) \equiv \begin{cases} x^3 - 3x - 1 & \pmod{2} \\ \cancel{(x+2)^3} & \pmod{3} \\ x^3 - 3x - 1 & \pmod{5} \\ x^3 - 3x - 1 & \pmod{7} \\ x^3 - 3x - 1 & \pmod{11} \\ x^3 - 3x - 1 & \pmod{13} \\ (x+7)(x+13)(x+14) & \pmod{17} \\ (x+3)(x+7)(x+9) & \pmod{19} \\ x^3 - 3x - 1 & \pmod{23} \\ x^3 - 3x - 1 & \pmod{24} \\ \quad \vdots & \end{cases}$$

It apears that the only reductions of F modulo p that we have are either irreducible or split (corresponding to the cycle types $(***)$ and $(*)$ respectively). This suggests that the Galois group is A_3, but from these calculations, there is no reason to assume that no other type of factorization will appear. This question is answered by the Chebotarev Density Theorem.

4 The Chebotarev Density Theorem

Definition. Let P denote the set of all finite primes of K and let $S \subseteq P$ and subset. We say that S has *Dirichlet density* δ if

$$\delta = \delta(S) = \lim_{X \to \infty} \frac{\#\{\mathfrak{p} \in S \mid N(\mathfrak{p}) \leq X\}}{\#\{\mathfrak{p} \in P \mid N(\mathfrak{p}) \leq X\}}$$

where $N(\mathfrak{p}) := \#(\mathcal{O}_K/\mathfrak{p})$ is the ideal norm of $\mathfrak{p}$.

Theorem 4.1. *(Chebotarev) Let $\mathcal{C}$ be a conjugacy class in G. Then the set*

$$\Xi = \Xi_{\mathcal{C}} = \{\mathfrak{p} \in P \mid (\mathfrak{p}, L/K) = \mathcal{C}\}$$

has Dirichlet density

$$\delta = \delta(\Xi_{\mathcal{C}}) = \frac{\#\mathcal{C}}{\#G}.$$

See Theorem 6.4 in chapter V of [Neu86] for a proof.

Remarks 4.2. (about the Chebotarev Density Theorem)

(4.2.1) If L/K is abelian, then $\#\mathcal{C} = 1$ for all conjugacy classes in G and thus $\delta(\Xi_{\mathcal{C}}) = 1/n$ for all conjugacy classes.

(4.2.2) If we set $\mathcal{C} = 1$, then $\delta(\Xi_{\mathcal{C}}) = 1/n$. In view of (2.1.4), this means that $\frac{1}{n}$ of all primes $\mathfrak{p}$ split completely in L. This yields another proof of the fact that infinitely many primes split completely.

(4.2.3) By a result of Lagarias and Odlyzko (see for example Theorem 1.1 of [MOL79]), there exists an absolute, effectively computable constant A (independent of K and L) such that for all conjugacy classes $\mathcal{C} \subseteq G$, there exists a prime ideal $\mathfrak{p}$ of K such that $(\mathfrak{p}, L/K) = \mathcal{C}$ and

$$N(\mathfrak{p}) \leq 2\Delta_L^A$$

where Δ_L is the number field discriminant of L/K. In words, this means that if a certain cycle type hasn't appeared as a Frobenius element of some $\mathfrak{p}$ for $N(\mathfrak{p}) \leq 2\Delta_L^A$, then it cannot appear at all.

Examples 4.3. (of the Chebotarev Density Theorem)

(4.3.1) If L/K is a quadratic extension, $G \cong (\mathbb{Z}/2\mathbb{Z})$ and thus there are only two conjugacy classes: $\mathcal{C} = \{1\}$ gives the primes that split completely by (2.1.4); $\mathcal{C} = \{-1\}$ then the Frobenius element is nontrivial and thus doesn't split so this gives primes that are inert (since theu must be unramified). In conclusion, $\frac{1}{2}$ of the primes of K split completely in L and the other $\frac{1}{2}$ remain inert.

(4.3.2) If $L = \mathbb{Q}(\zeta)$ is a cyclotomic extension, then $G \cong (\mathbb{Z}/m\mathbb{Z})^\times$ is abelian. By example (2.2.2), the Frobenius element/conjugacy class of the prime p is simply $p \pmod m \in (\mathbb{Z}/m\mathbb{Z})^\times$. Thus for each element of G, i.e. residue class modulo m, there are $1/\#(\mathbb{Z}/m\mathbb{Z})^\times$ many primes in that residue class. This is the celebrated Dirichlets Theorem on Primes in Arithmetic Progressions. Thus the Chebotarev Density Theorem generalizes Dirichlet's Theorem.

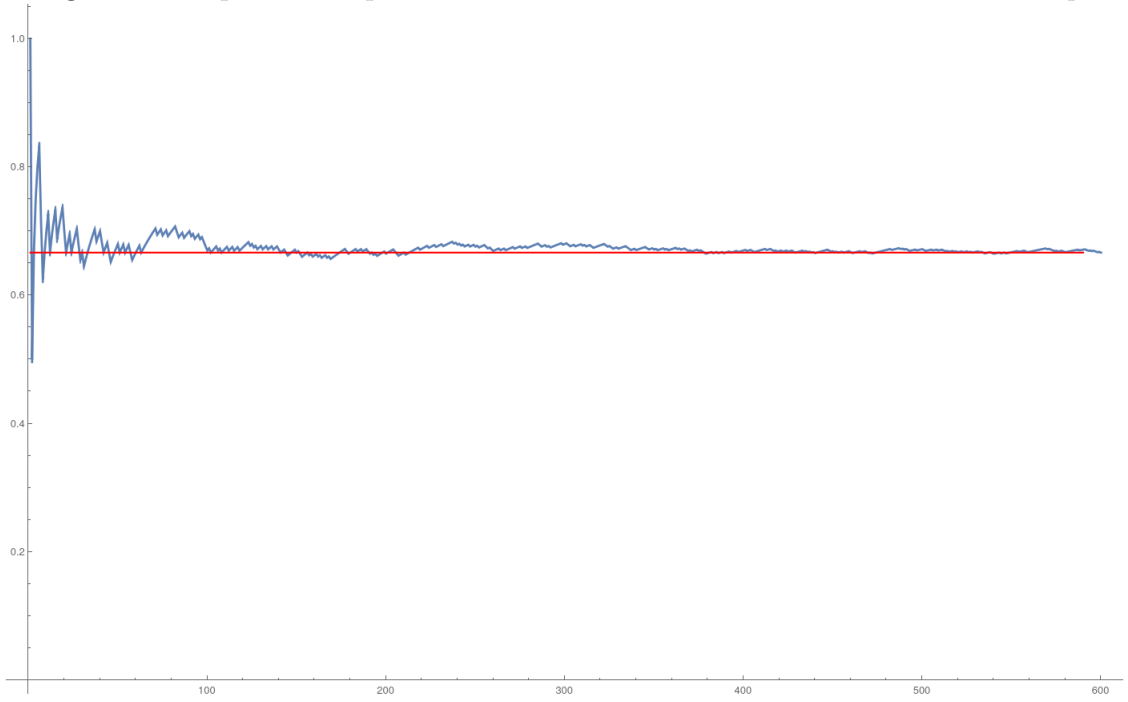
(4.3.3) If F is a cubic polynomial with coefficients in $\mathbb{Q}$, and L is the splitting field, then F will have the following behavior modulo primes:

- $(G = 1)$ F will split modulo all primes.
- $(G \cong C_2)$ F will split modulo $\frac{1}{2}$ of the primes and F will have an irreducible quadratic factor modulo $\frac{1}{2}$ of the primes p, corresponding to the cycle type $(p, L/\mathbb{Q}) = (**)$.
- $(G \cong A_3)$ F will split modulo $\frac{1}{3}$ of the primes and F will be irreducible modulo $\frac{2}{3}$ of the primes, corresponding to the cycle type $(p, L/\mathbb{Q}) = (***)$; there are two 3-cycles in A_3, each one corresponds to one conjugacy class of density $\frac{1}{3}$.

($G \cong S_4$) F will split modulo $\frac{1}{6}$ of the primes; will have a quadratic factor modulo $\frac{1}{2}$ of the primes; will remain irreducible modulo $\frac{1}{3}$ of the primes.

So if we reconsider $F(x) = x^3 - 3x - 1$ as in §3, and graph the proportion of primes p for which $F \pmod p$ is irreducible, we get Figure 1 below. By looking at the graph, we can see that the proportion of irreducible reductions tends to $\frac{2}{3}$ and thus we can comfortably guess that the Galois group is indeed A_3. In fact, if enough primes are checked, then Lagarias-Odlyzko will guarantee that $G \cong A_3$.

Figure 1: Proportion of primes for which $x^3 - 3x - 1$ is irreducible modulo p.



References

[DF04] D. Dummit and R. Foote. *Abstract Algebra*. John Wiley & Sons, 2004.

[Mil17] J. S. Milne. *Algebraic Number Theory*. 2017. Available at www.jmilne.org/math/.

[MOL79] H. L. Montgomery, A. M. Odlyzko, and J. C. Lagarias. A bound for the least prime ideal in the chebotarev density theorem. 1979.

[Neu86] J. Neukirch. *Class Field Theory*. Springer, 1986.

[Neu99] J. Neukirch. *Algebraic Number Theory*. Springer, 1999.