Some interesting consequences of Chebotarev density theorem

2025-12-13

Introduction

The aim of this post is to explain some of the consequences of Cebotarev density theorem.

First of all, we define the objects we need, see chapter 13 of Neukirch (1999).

Definition: Let K be a number field and L/K be a Galois extension with Galois group G. For every $\sigma \in G$ we define $P_{L|K}(\sigma)$ as the set of all unramified prime ideals $\mathfrak{p}$ of K such that there exists a prime ideal $\mathfrak{P}|\mathfrak{p}$ of L satisfying

$$\sigma = \Big(\frac{L|K}{\mathfrak{P}}\Big)$$

where $\left(\frac{L|K}{\mathfrak{P}}\right)$ is the Frobenius automorphism of $\mathfrak{P}$ over K.

Since for all $\tau \in G$ we have

$$\Big(\frac{L|K}{\tau\mathfrak{P}}\Big) = \tau\Big(\frac{L|K}{\mathfrak{P}}\Big)\tau^{-1}$$

the set $P_{L|K}(\sigma)$ only depends on the conjugacy class

$$\langle\sigma\rangle := \{\tau\sigma\tau^{-1} | \tau \in G\}$$

Moreover, if $\langle\sigma\rangle \neq \langle\tau\rangle$ then $P_{L|K}(\sigma) \cap P_{L|K}(\tau) = \emptyset$.

We now want to define what a density is.

Definition: Let $A \subseteq \mathbb{N}$. Set $A(n) := \{1, \dots, n\} \cap A$ and $a(n) := |A(n)|$. If the limit exists, we define the *natural density* $d(A)$ as

$$d(A) := \lim_{n\to\infty} \frac{a(n)}{n}$$

The theorem

We are now ready to state the theorem

Theorem 0.1 (Chebotarev density theorem)**.** *Let K be a number field and L/K be a finite Galois extension with Galois group G. Then for every $\sigma \in G$, the set $P_{L|K}(\sigma)$ has density (the limit exists), and it is given by*

$$d(P_{L|K}(\sigma)) = \frac{\#\langle\sigma\rangle}{\#G}$$

We will not prove Theorem 0.1, since the argument is long and technical. For a complete proof look at Neukirch (1999).

The consequences

We finally can learn about the corollaries of Theorem 0.1.

Characterization of number fields through splitting of primes

Definition: Let L/K be an extension of number fields and $\mathfrak{p}$ be a prime of K. We say that $\mathfrak{p}$ splits completely in L if for every prime $\mathfrak{P}|\mathfrak{p}$

$$f(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p}) = 1$$

where f is the inertia index and e is the ramification index. We define $P(L|K)$ as the set of primes of K splitting completely in L.

Corollary 0.1 (M. Bauer)**.** *Let K be a number field, L/K be a finite Galois extension, and M/K be a finite extension. Then*

$$P(M|K) \subseteq P(L|K) \iff L \subseteq M$$

Therefore,

$$P(M|K) = P(L|K) \iff L = M$$

i.e. the primes splitting completely completely determine the number field.

Proof. If $L \subseteq M$ then $P(M|K) \subseteq P(L|K)$ because of the multiplicativity of inertia and ramification index in towers of extensions. □

Neukirch, Jürgen. 1999. *Algebraic Number Theory.* 1st ed. Vol. 322. Grundlehren Der Mathematischen Wissenschaften. Berlin, Heidelberg: Springer-Verlag. https://doi.org/10.1007/978-3-662-03983-0.