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 recall some definition 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 you can look at Neukirch (1999).

The consequences

We finally can learn about the corollaries of Theorem 0.1.

There are infinitely many primes splitting completely

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

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

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 (of Theorem 0.1)**.** *Let K be a number field and L/K be a finite Galois extension. Then there are infinitely many primes of K splitting completely in L.*

Proof. Let $\mathfrak{p}$ be a prime of K. For the same reasoning used in the proof of Lemma 0.1 we have

$$\mathfrak{p} \text{ splits completely in } L \iff \left(\frac{L|K}{\mathfrak{P}}\right) = 1_G$$

Indeed, $\mathfrak{p}$ splits completely in L means that it is unramified and that its inertia index is 1. But this means that the decomposition group $D(\mathfrak{P}|\mathfrak{p})$ is trivial for every $\mathfrak{P}|\mathfrak{p}$. Since the Frobenius automorphism a generator of the group,

$$D(\mathfrak{P}|\mathfrak{p}) = \{1\} \iff \left(\frac{L|K}{\mathfrak{P}}\right) = 1_G$$

Therefore, we get that $P(L|K) = P_{L|K}(1_G)$. Applying Theorem 0.1 we obtain

$$d(P(L|K)) = \frac{1}{\#\mathrm{Gal}(L/K)} \neq 0$$

hence the set $P(L|K)$ must be infinite (otherwise its density would be 0. □

Characterization of number fields through splitting of primes

Lemma 0.1. *Let K be a number field, let L and M be two finite Galois extensions of K, and $N := LM$ the composite field. For every prime $\mathfrak{p}$ of K unramified in N, pick a prime $\mathfrak{P}$ of N above $\mathfrak{p}$. Then*

$$\mathfrak{p} \in P(M|K) \iff \left(\frac{N|K}{\mathfrak{P}}\right) \in H_M$$

Proof. Since M/K is Galois, the restriction map

$$\mathrm{res}_M : G = \mathrm{Gal}(N/K) \to \mathrm{Gal}(M/K)$$

is surjective with kernel H_M. Since $\mathfrak{p}$ is unramified, the Frobenius automorphism is well defined and it satisfies:

$$\mathrm{res}_M\left(\left(\frac{N|K}{\mathfrak{P}}\right)\right) = \left(\frac{M|K}{\mathfrak{P} \cap M}\right) \in \mathrm{Gal}(M/K)$$

Now observe that $\mathfrak{p}$ splits completely in M if and only if every prime of M above $\mathfrak{p}$ has inertia index 1 (since we already know that $\mathfrak{p}$ is unramified). Equivalently, (as seen in the proof of Corollary 0.1)

$$\left(\frac{M|K}{\mathfrak{P}}\right) = 1.$$

This holds if and only if $\left(\frac{N|K}{\mathfrak{P}}\right) \in \ker(\mathrm{res}_M) = H_M$. □

Proposition 0.1 (M. Bauer)**.** *Let K be a number field and let L and M be two finite Galois extensions of K. Then*

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

Therefore,

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

In other words, the primes splitting completely determine univocally 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.

Conversely, define the composite field $N := LM$ and set

$$G := \mathrm{Gal}(N/K), \quad H_L := \mathrm{Gal}(N/L), \quad H_M := \mathrm{Gal}(N/M).$$

Assume for the sake of contradiction that $L \not\subseteq M$. This is equivalent to $H_M \not\subseteq H_L$. Choose $g \in H_M \setminus H_L$. Since H_M and H_L are normal,

$$\langle g \rangle \subseteq H_M, \quad \langle g \rangle \cap H_L = \emptyset$$

By Theorem 0.1 there are infinitely many primes $\mathfrak{p}$ of K unramified in N with Frobenius conjugacy class equal to $\langle g \rangle$ (if it was finite, the density would be 0). For such a $\mathfrak{p}$, pick $\mathfrak{P}|\mathfrak{p}$ in N; then

$$\left(\frac{N|K}{\mathfrak{P}}\right) \in \langle g \rangle \subseteq H_M$$

By Lemma 0.1

$$\mathfrak{p} \in P(M|K)$$

But also $\left(\frac{N|K}{\mathfrak{P}}\right) \notin H_L$, so $\mathfrak{p} \notin P(L|K)$. This contradicts $P(M|K) \subseteq P(L|K)$. □

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.