Some interesting consequences of Chebotarev density theorem

2025-12-13

Introduction

First of all, we recall some definitions we need; see Chapter VII, §13 of Neukirch (1999).

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

$$\sigma = \mathrm{Frob}_{\mathfrak{P}}^{L|K},$$

where $\mathrm{Frob}_{\mathfrak{P}}^{L|K} \in G$ is the Frobenius automorphism of $\mathfrak{P}$ over $\mathfrak{p}$.

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

$$\mathrm{Frob}_{\tau\mathfrak{P}}^{L|K} = \tau \mathrm{Frob}_{\mathfrak{P}}^{L|K} \tau^{-1},$$

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

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

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 (for sets of primes of a number field).

Definition: Let K be a number field and let S be a set of nonzero prime ideals of $\mathcal{O}_K$. For $x \geq 1$ set

$$S(x) := \{\mathfrak{p} \in S \mid N\mathfrak{p} \leq x\}, \qquad \pi_S(x) := |S(x)|.$$

Let $\pi_K(x)$ be the number of all nonzero prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ with $N\mathfrak{p} \leq x$. If the limit exists, we define the *natural density* $d(S)$ as

$$d(S) := \lim_{x\to\infty} \frac{\pi_S(x)}{\pi_K(x)}.$$

The theorem

We are now ready to state the theorem.

Theorem 0.1 (Chebotarev density theorem)**.** *Let K be a number field and let 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 can finally look at some corollaries of Theorem 0.1.

There are infinitely many primes splitting completely

Definition: Let L/K be a finite extension of number fields of degree n and let $\mathfrak{p}$ be a prime of K. We say that $\mathfrak{p}$ splits completely in L if the number of (distinct) prime ideals of L lying over $\mathfrak{p}$ is exactly n. We define $P(L|K)$ as the set of primes of K splitting completely in L.

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

Proof. First, suppose that L/K is Galois. Let $\mathfrak{p}$ be a prime of K unramified in L, and let $\mathfrak{P}|\mathfrak{p}$ in L. Then

$$\mathfrak{p} \text{ splits completely in } L \iff \mathrm{Frob}_{\mathfrak{P}}^{L|K} = 1_G.$$

Indeed, $\mathfrak{p}$ splits completely means that for every $\mathfrak{P}|\mathfrak{p}$ we have $e(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = 1$ (respectively ramification index and residue degree), hence the decomposition group $D(\mathfrak{P}|\mathfrak{p})$ is trivial. Since $\mathfrak{p}$ is unramified, the decomposition group is cyclic and generated by the Frobenius element, so

$$D(\mathfrak{P}|\mathfrak{p}) \text{ is trivial} \iff \mathrm{Frob}_{\mathfrak{P}}^{L|K} = 1_G.$$

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

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

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

If L/K is not Galois, let M be the Galois closure of L over K. By the Galois case, $P(M|K)$ is infinite. Moreover $P(M|K) \subseteq P(L|K)$ by multiplicativity of residue degrees and ramification indices in towers. Hence $P(L|K)$ is infinite as well. □

Characterization of number fields (Galois over K) 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. Set*

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

For every prime $\mathfrak{p}$ of K unramified in N, pick a prime $\mathfrak{P}$ of N above $\mathfrak{p}$. Then

$$\mathfrak{p} \in P(M|K) \iff \mathrm{Frob}_{\mathfrak{P}}^{N|K} \in H_M.$$

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 in N, the Frobenius element is well-defined and it satisfies

$$\mathrm{res}_M(\mathrm{Frob}_{\mathfrak{P}}^{N|K}) = \mathrm{Frob}_{\mathfrak{P}\cap M}^{M|K} \in \mathrm{Gal}(M/K).$$

Now observe that $\mathfrak{p}$ splits completely in M if and only if the Frobenius element in $\mathrm{Gal}(M/K)$ is trivial:

$$\mathfrak{p} \in P(M|K) \iff \mathrm{Frob}_{\mathfrak{P}\cap M}^{M|K} = 1.$$

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

Corollary 0.2 (M. Bauer, corollary of Theorem 0.1)**.** *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,

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

Remark 0.1. The implication $P(M|K) \subseteq P(L|K) \Rightarrow L \subseteq M$ can be strengthened by allowing finitely many primes in $P(M|K)$ not to lie in $P(L|K)$; the proof remains unchanged.

Proof. If $L \subseteq M$ then $P(M|K) \subseteq P(L|K)$ because in a tower the ramification indices and residue degrees are multiplicative.

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

$$\mathrm{Frob}_{\mathfrak{P}}^{N|K} \in \langle g \rangle \subseteq H_M.$$

By Lemma 0.1 we get $\mathfrak{p} \in P(M|K)$.

Similarly, $\mathfrak{p} \in P(L|K)$ would imply $\mathrm{Frob}_{\mathfrak{P}}^{N|K} \in H_L$, which is false here. Hence $\mathfrak{p} \notin P(L|K)$. This contradicts $P(M|K) \subseteq P(L|K)$.

Therefore $L \subseteq M$. □

Dirichlet's Theorem on primes in arithmetic progressions

Corollary 0.3 (Dirichlet's Theorem)**.** *Let $a, n \geq 1$ be integers with $\gcd(a, n) = 1$. Then there are infinitely many primes such that $p \equiv a \pmod{n}$.*

Proof. Let ζ be a primitive n-th root of unity, define $L := \mathbb{Q}(\zeta)$, and let $G := \mathrm{Gal}(L/\mathbb{Q})$. We know that $L/\mathbb{Q}$ is Galois and

$$G \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

where the class of b corresponds to the automorphism sending ζ to ζ^b.

Let p be a prime with $p \nmid n$. Then p is unramified in L, and for any prime $\mathfrak{P}|p$ in L the Frobenius automorphism satisfies

$$\mathrm{Frob}_{\mathfrak{P}}^{L|\mathbb{Q}}(\zeta) = \zeta^p.$$

In other words, under the isomorphism $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$, the Frobenius element corresponds to the class of p mod n.

Therefore,

$$p \equiv a \pmod{n} \quad \iff \quad \mathrm{Frob}_{\mathfrak{P}}^{L|\mathbb{Q}} \text{ corresponds to } a \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

By Theorem 0.1, the set of such primes has positive density, hence it is infinite. (The finitely many primes dividing n are irrelevant.) □

Condition for linearity of a polynomial

Corollary 0.4. *Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial such that for all but finitely many primes p the reduction $\bar{f} \in \mathbb{F}_p[X]$ has a root. Then* $\deg(f) = 1$.

Proof. Let $n := \deg(f)$ and suppose that $n > 1$. Let L be the splitting field of f over $\mathbb{Q}$ and set $G := \mathrm{Gal}(L/\mathbb{Q})$. Let Ω be the set of roots of f in L. Since f is irreducible, the action of G on Ω is transitive. By Burnside's lemma (orbit-counting), there is some $\sigma \in G$ with no fixed points in Ω.

Let S be a finite set of rational primes containing all primes ramified in the splitting field L, and also containing all primes dividing $\mathrm{Disc}(f)$ or the leading coefficient of f. For every $p \notin S$, the reduction $(f \bmod p)$ is separable, and p is unramified in the splitting field L. Moreover, the factorization type of $(f \bmod p)$ corresponds to the cycle structure of $\mathrm{Frob}_{\mathfrak{P}}^{L|\mathbb{Q}}$ acting on Ω, where $\mathfrak{P}|p$. In particular, $(f \bmod p)$ has a root in $\mathbb{F}_p$ if and only if $\mathrm{Frob}_{\mathfrak{P}}^{L|\mathbb{Q}}$ has a fixed point in Ω.

By Theorem 0.1, the set $P_{L|\mathbb{Q}}(\sigma)$ is infinite (it has positive density). Since S is finite, there are infinitely many primes $p \notin S$ such that

$$\mathrm{Frob}_{\mathfrak{P}}^{L|\mathbb{Q}} \in \langle \sigma \rangle,$$

where $\mathfrak{P}|p$. For all such primes the Frobenius automorphism has no fixed points, thus the reduction of f has no roots modulo these primes. This is a contradiction, since we assumed that $(f \bmod p)$ has a root for all but finitely many primes.

Therefore $\deg(f) = 1$. □

How many $\mathbb{F}_p$-points?

Corollary 0.5. *Let A be a $\mathbb{Z}$-algebra of finite type such that there exists a ring map $f : A \to \mathbb{C}$. Then for infinitely many primes p there is a ring morphism $A \to \mathbb{F}_p$.*

What we are saying is that if you consider a set of polynomials in $\mathbb{Z}[X_1, \dots, X_n]$ (the polynomials defining A as a quotient of $\mathbb{Z}[X_1, \dots, X_n]$), then if they have a common solution in $\mathbb{C}$ (i.e. there is a map $A \to \mathbb{C}$), they have a common solution modulo p, for infinitely many primes p (i.e. a map $A \to \mathbb{F}_p$).

Proof. Since we have a map $f : A \to \mathbb{C}$, we get $A \otimes_{\mathbb{Z}} \mathbb{C} \neq 0$, which is equivalent to $A \otimes_{\mathbb{Z}} \mathbb{Q} \neq 0$ (because $\mathbb{Q} \to \mathbb{C}$ is faithfully flat). In particular, $A \otimes_{\mathbb{Z}} \mathbb{Q}$ has a maximal ideal $\mathfrak{m}$. Let

$$L := (A \otimes_{\mathbb{Z}} \mathbb{Q})/\mathfrak{m}.$$

By Zariski's lemma, L is a finite extension of $\mathbb{Q}$, hence a number field.

Consider now the composition map $\phi : A \to A \otimes_{\mathbb{Z}} \mathbb{Q} \to L$. Let $a_1, \dots, a_r$ be generators of A as a $\mathbb{Z}$-algebra. Choose $N \in \mathbb{Z}_{>0}$ such that $N \cdot \phi(a_i)$ is an algebraic integer for every $i = 1, \dots, r$. Then $\phi(a_i) \in \mathcal{O}_L[1/N]$ for all i, hence ϕ lands in $\mathcal{O}_L[1/N]$, i.e. we have a map

$$\phi : A \to \mathcal{O}_L[1/N].$$

Fix a rational prime p not dividing N. Any prime ideal $\mathfrak{P}$ of L dividing p gives the reduction map

$$\mathcal{O}_L[1/N] \to \mathcal{O}_L/\mathfrak{P}.$$

Moreover, if the residue degree satisfies $f(\mathfrak{P}|p) = 1$, then $\mathcal{O}_L/\mathfrak{P} \cong \mathbb{F}_p$, hence we get a map

$$A \to \mathcal{O}_L[1/N] \to \mathcal{O}_L/\mathfrak{P} \cong \mathbb{F}_p.$$

Since $p \nmid N$, this is the same as a map $A \to \mathbb{F}_p$.

By Corollary 0.1 there are infinitely many primes p splitting completely in L. Discarding the finitely many primes dividing N, we can assume also $p \nmid N$. This gives a map $A \to \mathbb{F}_p$ for infinitely many primes p. □

Conclusion

In this post we saw how the Chebotarev density theorem can be used as a very efficient "machine" to produce arithmetic information.

Starting from the simple observation that Frobenius elements encode splitting behaviour, we deduced that totally split primes always exist in abundance (in fact with positive density), and we used this to prove a rigidity statement: in the Galois case, knowing which primes split completely already determines the extension.

We also proved Dirichlet's theorem on primes in arithmetic progressions by applying Chebotarev to cyclotomic fields, and we saw a typical application to polynomials: if an irreducible polynomial has a root modulo almost every prime, then it must be linear.

All these results share the same pattern: translate a question into a condition on Frobenius conjugacy classes, then use Chebotarev to conclude that the relevant primes not only exist, but are infinitely many.

I would like to thank my friend who suggested this topic to me and helped me write this post.

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.