Prime decomposition in Galois case and Cebotarev theorem

Tuan Dung Hoang

December 18, 2025

Consider K is a number field.

From previous lecture, we know that $\mathcal{O}_K$ is a Dedekind domain. If $p \in \mathbb{Z}$ is a nonzero prime, we want to see how $p\mathcal{O}_K$ decomposes in a product of prime ideals of $\mathcal{O}_K$.

We propose a few lemmas before proving the main theorem.

Lemma 1. *$p\mathcal{O}_K \neq \mathcal{O}_K$.*

Proof. If $1 \in p\mathcal{O}_K$ then $1 = p \cdot s$ for some $s \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, so $p \mid 1$, which is absurd. □

Let

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

be the decomposition of $p\mathcal{O}_K$ into a product of prime ideals of $\mathcal{O}_K$. Because this is a property of Dedekind domains, the $\mathfrak{p}_i$ (for $i = 1, \ldots, g$) are exactly all prime ideals of $\mathcal{O}_K$ lying over p.

The integers e_i are called the *ramification indices*, and

$$f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$$

is called the *inertia degree*.

Lemma 2. *For any $a \geqslant 1$,*

$$\dim_{\mathbb{F}_p}\left(\mathfrak{p}_i^a/\mathfrak{p}_i^{a+1}\right) = f_i.$$

Proof. Choose $s \in \mathfrak{p}_i^a \backslash \mathfrak{p}_i^{a+1}$. Consider the map

$$\mathcal{O}_K \longrightarrow \mathfrak{p}_i^a/\mathfrak{p}_i^{a+1}, \qquad b \longmapsto sb \bmod \mathfrak{p}_i^{a+1}.$$

This map has kernel $\mathfrak{p}_i$ (This map is $\mathcal{O}_K$-linear, so its kernel is an ideal of $\mathcal{O}_K$. It clearly contains $\mathfrak{p}_i$, but not 1 by choice of s. As $\mathfrak{p}_i$ is a maximal ideal, the kernel is $\mathfrak{p}_i$) and also from

$$\mathfrak{p}_i^{a+1} + (s) \subseteq \mathfrak{p}_i^a$$

we have $\mathfrak{p}_i^{a+1} + (s) = \mathfrak{p}_i^a$, so this map is surjective.

So

$$\mathcal{O}_K/\mathfrak{p}_i \cong \mathfrak{p}_i^a/\mathfrak{p}_i^{a+1}$$

so

$$\dim_{\mathbb{F}_p}(\mathfrak{p}_i^a/\mathfrak{p}_i^{a+1}) = f_i.$$

□

Our main theorem is:

Theorem 3. *If $n = [K : \mathbb{Q}]$ then*

$$n = \sum_{i=1}^{g} e_i f_i.$$

Proof. We have

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}.$$

By the Chinese remainder theorem we have

$$\mathcal{O}_K/(p)\mathcal{O}_K \cong \prod_{i=1}^{g} \mathcal{O}_K/\mathfrak{p}_i^{e_i}.$$

We have

$$\dim_{\mathbb{F}_p}\big(\mathcal{O}_K/(p)\mathcal{O}_K\big) = n \tag{1}$$

from $\#\,\mathcal{O}_K/(p)\mathcal{O}_K = p^n$
(As the underlyng abelian group of $\mathcal{O}_K$ is free of rank n, we have $|\mathcal{O}_K/p\mathcal{O}_K| = p^n$)

Meanwhile

$$\dim_{\mathbb{F}_p}\big(\mathcal{O}_K/\mathfrak{p}_i^{e_i}\big) = \sum_{a=0}^{e_i-1} \dim_{\mathbb{F}_p}\big(\mathfrak{p}_i^a/\mathfrak{p}_i^{a+1}\big) = e_i \cdot f_i \tag{2}$$

using Lemma 2.

From (1) and (2) we have

$$n = \sum_{i=1}^{g} e_i f_i.$$

□

In fact the theorem also true for L/K is finite extesion of number fields. In this case we consider $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $\mathfrak{p}\mathcal{O}_L$ factor as product of prime divisor:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

Put $f_i = [\mathcal{O}_L/\mathfrak{p}_i : \mathcal{O}/\mathfrak{p}]$ be inertia degree. We still have $[L : K] = \sum_{i=1}^{g} e_i f_i$. We will use this strong version to prove lemma 8 below. The detailed proof can be see in [**?**]
We will compute some easy examples and propose a lemma that let us know easier about the decomposition in case

$$\mathcal{O}_K = \mathbb{Z}[\alpha] \quad (\alpha \in \mathcal{O}_K) \quad \text{(monogeneous)}.$$

Example: $K = \mathbb{Q}(\sqrt{d})$ with d a square-free integer. Then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4, \\ \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

If α is an algebraic integer such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ then let Π_α denote the minimal polynomial of α (take Π_α monic). We know $\Pi_\alpha \in \mathbb{Z}[x]$ and in fact $\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(\Pi_\alpha)$ (since for every $f \in \mathbb{Z}[x]$, $f = h \cdot \Pi_\alpha + g$ for some $g \in \mathbb{Z}[x]$, $\deg g < \deg \Pi_\alpha$).

In this case we have:

Lemma 4. *If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and Π_α is defined by assumption as above, then if we consider $\overline{\Pi}_\alpha$ the image of Π_α in $\mathbb{F}_p[x]$ and*

$$\overline{\Pi}_\alpha = \overline{P}_1^{e_1} \cdots \overline{P}_g^{e_g}$$

the factorization of $\overline{\Pi}_\alpha$ in $\mathbb{F}_p[x]$ into prime factors, then we have

$$(p)\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

where $\mathfrak{p}_i = (p)\mathcal{O}_K + P_i(\alpha)\mathcal{O}_K$ are different prime ideals above p, and the inertia degree f_i of $\mathfrak{p}_i$ is the degree of $\overline{P}_i$.

Proof. Omitted. □

In case $K/\mathbb{Q}$ is a Galois extension.

Denote $G = \mathrm{Gal}(K/\mathbb{Q})$. Then $\sigma(\mathcal{O}_K) = \mathcal{O}_K$ for all $\sigma \in G$ (since σ preserves coefficients of polynomials).

For $\mathfrak{p}_i \subset \mathcal{O}_K$ a prime ideal, σ induces an isomorphism between

$$\mathcal{O}_K/\mathfrak{p}_i \xrightarrow{\cong} \mathcal{O}_K/\sigma(\mathfrak{p}_i).$$

From this we have $\sigma(\mathfrak{p}_i)$ is also a prime ideal of $\mathcal{O}_K$.

Since $\sigma(p) = p$ for a prime $p \in \mathbb{Z}$, $p > 0$,

$$\sigma(p)\mathcal{O}_K = p\mathcal{O}_K.$$

So $S = \{\mathfrak{p}_i \subset \mathcal{O}_K \mid \mathfrak{p}_i \text{ prime ideal}, \ p \in \mathfrak{p}_i\}$ is G-stable. Since $p \in \mathfrak{p}_i$ then $p \in \sigma(\mathfrak{p}_i)$, so $\sigma(\mathfrak{p}_i)$ is a prime ideal lying above p.

Our theorem is:

Theorem 5. *G acts transitively in S.*

Proof. If $\mathfrak{p}_i \neq \mathfrak{p}_j$ are two prime ideals above p, suppose $\sigma(\mathfrak{p}_i) \neq \mathfrak{p}_j$ for any $\sigma \in G$.

By Chinese remainder theorem, there exists $x \in \mathcal{O}_K$ such that

$$x \equiv 0 \pmod{\mathfrak{p}_j}, \qquad x \equiv 1 \pmod{\sigma(\mathfrak{p}_i)} \ \ \forall\, \sigma \in G.$$

Then

$$N_{K/\mathbb{Q}}(x) = \prod_{\sigma \in G} \sigma(x) \in \mathfrak{p}_j \cap \mathbb{Z} = (p),$$

on the other hand $x \notin \sigma(\mathfrak{p}_i)$ for all $\sigma \in G$, so

$$\sigma(x) \notin \mathfrak{p}_i \quad \forall\, \sigma \in G$$

and hence

$$\prod_{\sigma \in G} \sigma(x) \notin \mathfrak{p}_i \cap \mathbb{Z} = (p),$$

a contradiction. □

From theorem 5 we deduce:

Corollary 6. *If $K/\mathbb{Q}$ is a Galois extension then*

$$e_1 = \cdots = e_g = e, \qquad f_1 = \cdots = f_g = f,$$

and $efg = n$ (where $n = [K : \mathbb{Q}]$).

Proof. It follows from the isomorphisms

$$\mathcal{O}_K/\mathfrak{p}_i \cong \mathcal{O}_K/\sigma(\mathfrak{p}_i)$$

so $f_i = f$ for all i, and from properties of Dedekind domains, so $e_i = e$ for all i. □

Moreover, Theorem 5 and Corollary 6 are also true for L/K is finite Galois extension of number fields and we will use this general form in proof of lemme 8.

Definition 7. If $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$ then the subgroup

$$G_{\mathfrak{p}} = \{\sigma \in G \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

is called the *decomposition group* of $\mathfrak{p}$ over $\mathbb{Q}$. The fixed field

$$Z_{\mathfrak{p}} = \{x \in K \mid \sigma x = x \ \forall\, \sigma \in G_{\mathfrak{p}}\}$$

is called the *decomposition field* of $\mathfrak{p}$ over K.

Corollary 6 means that the decomposition of (p) in $\mathcal{O}_K$ has the following form in the Galois case:

$$(p)\mathcal{O}_K = \Big(\prod_{\sigma} \sigma\mathfrak{p}_1\Big)^e$$

where σ varies over a system of representatives of $G/G_{\mathfrak{p}_1}$. We have lemma 8:

Lemma 8. *Let $\mathfrak{p}_{1,Z} = \mathfrak{p}_1 \cap Z_{p_1}$ be a prime ideal of Z_{p_1} below $\mathfrak{p}_1$. Then we have:*

(i) $\mathfrak{p}_{1,Z}$ has only one prime lying above it, namely $\mathfrak{p}_1$.

(ii) $\mathfrak{p}_1$ over $\mathfrak{p}_{1,Z}$ has ramification index e and inertia degree f.

(iii) The ramification index and inertia degree of $\mathfrak{p}_{1,Z}$ over $\mathbb{Q}$ are both equal to 1.

Proof. (i) $\mathrm{Gal}(K/Z_{p_1}) = G_{\mathfrak{p}_1}$, so from Lemma 5, $\mathfrak{p}_1$ is the only prime lying above $\mathfrak{p}_1$.

(ii) $\#G_{\mathfrak{p}_1} = [K : Z_{p_1}] = ef$. Let e' and e'' be the ramification indices of $\mathfrak{p}_1$ over $Z_{\mathfrak{p}_1}$ and $\mathfrak{p}_{1,Z}$ over $\mathbb{Q}$

$$\mathfrak{p}Z_{p_1} = \mathfrak{p}_{1,Z}^{e''}\ldots \quad \text{and} \quad \mathfrak{p}_{1,Z} = \mathfrak{p}_1^{e'}.$$

Then $e = e'e''$. Similarly, $f = f'f''$.

Theorem 3 implies

$$[K : Z_{p_1}] = e'f',$$

so $e'f' = ef$ and hence $e'' = f'' = 1$.

(iii) Therefore the ramification index and inertia degree of $\mathfrak{p}_{1,Z}$ over $\mathbb{Q}$ are both equal to 1.

Since $\sigma(\mathcal{O}_K) = \mathcal{O}_K$ and $\sigma(\mathfrak{p}_1) = \mathfrak{p}_1$ for all $\sigma \in G_{\mathfrak{p}_1}$, σ induces an automorphism

$$\mathcal{O}_K/\mathfrak{p}_1 \to \mathcal{O}_K/\mathfrak{p}_1, \qquad a \bmod \mathfrak{p}_1 \mapsto \sigma(a) \bmod \mathfrak{p}_1.$$

□

Put $k(\mathfrak{p}_1) = \mathcal{O}_K/\mathfrak{p}_1$, $k(p) = \mathbb{F}_p$.

We have:

Lemma 9. *The canonical map*

$$G_{\mathfrak{p}_1} \longrightarrow \mathrm{Gal}\big(k(\mathfrak{p}_1)/\mathbb{F}_p\big)$$

is surjective.

Proof. The inertia degree of $\mathfrak{p}_{1,Z}$ over $\mathbb{Q}$ is 1 (Lemma 8). Z_{p_1} and $\mathbb{Q}$ have the same residue class field with respect to p.

Assume $Z_{p_1} = \mathbb{Q}$, $G_{\mathfrak{p}_1} = G$. Let $\overline{\theta}$ be a primitive element for $k(\mathfrak{p}_1)/k(p)$. Let $\overline{\sigma} \in \mathrm{Gal}\big(k(\mathfrak{p}_1)/k(p)\big)$.

Write $\theta \in \mathcal{O}_K$ a representative of $\overline{\theta}$ over $\mathbb{Q}$, and let $f(x), g(x)$ be the minimal polynomials of θ over $\mathbb{Q}$ and of $\overline{\theta}$ over $\mathbb{F}_p$ respectively. Then $\overline{g}(x)$ divides $\overline{f}(x)$, so $\overline{\sigma}\,\overline{\theta}$ is a root of $\overline{f}(x)$. Using $K/\mathbb{Q}$ is Galois, so f split completely in $\mathbb{Q}$. So there exists θ' a zero of $f(x)$ such that

$$\overline{\theta}' = \overline{\sigma}\,\overline{\theta} \pmod{\mathfrak{p}_1}.$$

Then $\theta' = \sigma(\theta)$ for some $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ (if $K/\mathbb{Q}$ is Galois then G is transitive on the set of roots as above).

So σ maps to $\overline{\sigma}$. □

Definition 10. Let $\ker I_{\mathfrak{p}_1} \subset G_{\mathfrak{p}_1}$ be the kernel of the homomorphism

$$G_{\mathfrak{p}_1} \longrightarrow \mathrm{Gal}\big(k(\mathfrak{p}_1)/\mathbb{F}_p\big).$$

Then $I_{\mathfrak{p}_1}$ is called the *inertia group* of $\mathfrak{p}_1$ over $\mathbb{Q}$.

We have $\#I_{\mathfrak{p}_1} = e$. In fact, in almost all $p \in \mathbb{Z}$ (those p which do not divide $\mathrm{disc}(K)$) the prime p is unramified over $\mathbb{Q}$ (i.e. $e = 1$).

So in the case p unramified,

$$G_{\mathfrak{p}_1} \cong \mathrm{Gal}\big(k(\mathfrak{p}_1)/\mathbb{F}_p\big)$$

a cyclic group generated by a Frobenius element.

There exists a unique $\varphi_{\mathfrak{p}_1} \in \mathrm{Gal}(K/\mathbb{Q})$ such that

$$\varphi_{\mathfrak{p}_1}(a) \equiv a^N \pmod{\mathfrak{p}_1} \quad \text{for all } a \in \mathcal{O}_K,$$

where $N = [k(\mathfrak{p}_1) : \mathbb{F}_p]$.

$G_{\mathfrak{p}_1}$ is cyclic in this case and $\varphi_{\mathfrak{p}_1}$ is generated by $\mathfrak{p}_1$.

In the next part, we will discuss the Chebotarev density theorem and its relation with Dirichlet's theorem for primes in arithmetic progression.

Before stating the Chebotarev theorem, we have the following notation.

Definition 11. Let M be a set of prime ideals of $\mathcal{O}_K$. The limit

$$d(M) = \lim_{s \to 1^+} \frac{\sum\limits_{\mathfrak{p} \in M} N(\mathfrak{p})^{-s}}{\sum\limits_{\mathfrak{p}} N(\mathfrak{p})^{-s}},$$

if it exists, is called the *Dirichlet density* of M.

For $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$

Consider the set $P_{K/\mathbb{Q}}(\sigma)$ of all unramified prime ideals p of $\mathbb{Q}$ such that there exists $\mathfrak{p}_1 \in \mathcal{O}_K$ with $p \mid \mathfrak{p}_1$ satisfying

$$\sigma = \left(\frac{K/\mathbb{Q}}{\mathfrak{p}_1}\right),$$

the Frobenius automorphism $\varphi_{\mathfrak{p}_1}$ of $\mathfrak{p}_1$ over $\mathbb{Q}$.

This set depends only on the conjugacy class

$$\langle\sigma\rangle = \{\tau\sigma\tau^{-1} \mid \tau \in \mathrm{Gal}(K/\mathbb{Q})\}.$$

Theorem 12 (Chebotarev)**.** *Let $K/\mathbb{Q}$ be a Galois extension with group G. For every $\sigma \in G$, $P_{K/\mathbb{Q}}(\langle\sigma\rangle)$ has a density*

$$d\big(P_{K/\mathbb{Q}}(\langle\sigma\rangle)\big) = \frac{\#\langle\sigma\rangle}{\#G}.$$

Using this theorem, we can deduce Dirichlet's theorem.

Consider $n > 1$, $n \in \mathbb{Z}$. Let $\varepsilon = e^{2\pi i/n}$ be an n-th primitive root of unity.

We know that $k = \mathbb{Q}(\varepsilon)/\mathbb{Q}$ is a Galois extension with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times \cong G$ via

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\delta} G, \qquad \delta : m \longmapsto (\varepsilon \mapsto \varepsilon^m), \quad (m, n) = 1.$$

Since the group G is abelian, for $(a, n) = 1$

$$d\big(P_{K/\mathbb{Q}}(f(a))\big) = \frac{1}{\varphi(n)}.$$

Recall that $\mathcal{O}_K = \mathbb{Z}[\varepsilon]$ and p is unramified in K if and only if $p \nmid n$ (using Lemma 9). We can also prove that almost except finite p belong to $P_{K/\mathbb{Q}}(f(a))$ is $p \equiv a(mod n)$. From this aspect, we can prove the following theorem.

Theorem 13 (Dirichlet)**.** *If $(a, n) = 1$ then the arithmetic progression*

$$a + nb, \quad b = 1, 2, \ldots$$

contains infinitely many prime numbers. The Dirichlet density of these primes is $1/\varphi(n)$