

HW #11

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Reading Homework. Try Exercises 5.3, 5.4, 5.5, 5.6 in the textbook. Read the solutions in the back.

Question 1. Let K be a number field. Let p be a rational prime that is unramified in K .

- (1) Suppose that $K/\mathbb{Q}$ is Galois. Show that

There exists $\alpha \in \mathcal{O}_K$ such that $p = |N_{K/\mathbb{Q}}(\alpha)| \Leftrightarrow p$ splits completely in H_K .

- (2) Suppose that $K/\mathbb{Q}$ is Galois. Suppose that K is **totally imaginary** (i.e., all archimedean primes of K are complex). Show that

There exists $\alpha \in \mathcal{O}_K$ such that $p = N_{K/\mathbb{Q}}(\alpha) \Leftrightarrow p$ splits completely in H_K .

- (3) Show that, in general, only one direction of the equivalence in Question 1(1) is true.

- (4) Find a counterexample to the other direction in Question 1(1) when $K/\mathbb{Q}$ is not Galois as follows.

- (a) Let $K = \mathbb{Q}(\sqrt[3]{3})$. Show that $h_K = 1$.

Hint. By Example 2.15, you know $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{3}]$. Use Minkowski bound.

- (b) Find p such that the prime ideal factorization of (p) in K is given by

$$(p) = \mathfrak{p}_1 \mathfrak{p}_2, \quad f(\mathfrak{p}_1|p) = 1, \quad f(\mathfrak{p}_2|p) = 2.$$

- (c) Deduce that this gives a counterexample.

- (5) Suppose that $K/\mathbb{Q}$ is Galois. Let H_K^+ be the **narrow Hilbert class field of K** ; namely, $H_K^+ := K(\mathfrak{m})$ is the ray class field of modulus $\mathfrak{m} = \mathfrak{m}_f \mathfrak{m}_\infty$ where $\mathfrak{m}_f = (1)$ and $\mathfrak{m}_\infty$ is the product of all real embeddings of K . Show that (note there is only one direction!)

There exists $\alpha \in \mathcal{O}_K$ such that $p = N_{K/\mathbb{Q}}(\alpha) \Leftrightarrow p$ splits completely in H_K^+ .

Question 2. Let K be a number field. Suppose that a rational prime p is inert in H_K . Show that $h_K = 1$ (i.e., $H_K = K$).

Question 3. We will study when a number is a fourth power (a **quartic residue**) modulo a rational prime, governed by what is called the **quartic reciprocity law**. Let p be a rational prime.

- (1) Suppose that $p \equiv 3 \pmod{4}$. Show that every quadratic residue mod p is a quartic residue mod p (i.e., if an integer a is a square mod p , it is a fourth power mod p).

Hint. For any integer b , either b or $-b$ is a quadratic residue mod p .

- (2) Let $K = \mathbb{Q}(\sqrt{-1})$, which contains $\mu_4 = \{\pm 1, \pm\sqrt{-1}\}$. Note that $h_K = 1$, so that any ideal of $\mathcal{O}_K$ is principal. Let $\pi = 1 - \sqrt{-1}$, which generates the unique prime ideal $\mathfrak{p}_2 = (\pi)$ of K dividing 2.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ that divides a rational prime $p \equiv 1 \pmod{4}$. Show that there exists a unique generator of $\mathfrak{p}$ congruent to 1 $\pmod{\pi^3}$. We call such a generator a **primary number**.

Hint. Show that $\mathcal{O}_K^\times = \mu_4$.

- (3) Let π_1, π_2 be primary numbers of K coprime to each other. If either π_1 or π_2 is further congruent to 1 $\pmod{4}$, show that

$$(\pi_1, \pi_2)_{\mathfrak{p}_2} = 1.$$

Hint. Adapt the proof of Exercise 5.6. Note that π is a uniformizer of $K_{\mathfrak{p}_2}$, and $4\mathcal{O}_K = \pi^4\mathcal{O}_K$.

- (4) Consider the 4-th power residue symbol $(\cdot) \in \mu_4$ (see Definition 5.46). Let π_1, π_2 be primary numbers of K coprime to each other. If either π_1 or π_2 is further congruent to 1 $\pmod{4}$, show that

$$\left(\frac{\pi_1}{\pi_2}\right) = \left(\frac{\pi_2}{\pi_1}\right).$$

- (5) Let π_1, π_2 be primary numbers of K coprime to each other. If both π_1 and π_2 are congruent to $3 + 2\sqrt{-1} \pmod{4}$, show that

$$\left(\frac{\pi_1}{\pi_2}\right) = -\left(\frac{\pi_2}{\pi_1}\right).$$

Hint. First show that this follows from $(3 + 2\sqrt{-1}, 3 + 2\sqrt{-1})_{\mathfrak{p}_2} = -1$. Use Hilbert reciprocity law to show that $(3 + 2\sqrt{-1}, 3 + 2\sqrt{-1})_{\mathfrak{p}_2} = (3 + 2\sqrt{-1}, 3 + 2\sqrt{-1})_{\mathfrak{p}_{13}}$, where $\mathfrak{p}_{13} = (3 + 2\sqrt{-1})$. Compute $(3 + 2\sqrt{-1}, 3 + 2\sqrt{-1})_{\mathfrak{p}_{13}}$ using Theorem 5.44.

- (6) (**Gauss's quartic reciprocity law**) Show that (4) and (5) can be neatly packaged into the following statement: if π_1, π_2 are primary numbers of K coprime to each other,

$$\left(\frac{\pi_1}{\pi_2}\right) = (-1)^{\frac{N_{K/\mathbb{Q}}(\pi_1)-1}{4} \cdot \frac{N_{K/\mathbb{Q}}(\pi_2)-1}{4}} \left(\frac{\pi_2}{\pi_1}\right).$$