

## HW #7

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

**Reading Homework.** Try Exercises A.6, A.7, A.8 in the textbook. Read its solutions in the back.

**Question 1.** (Do not use §4.3-4.5!)

(1) Let  $A$  be a Dedekind domain. Show that there is a one-to-one correspondence

$$\begin{aligned} \{\text{Nonzero prime ideals of } A\} &\leftrightarrow \left\{ \begin{array}{l} \text{Normalized discrete valuations } v \text{ on} \\ \text{Frac}(A) \text{ such that } v(x) \geq 0 \text{ for all } x \in A \end{array} \right\} \\ \mathfrak{p} \subset A &\mapsto v_{\mathfrak{p}} \text{ induced by the DVR } A_{\mathfrak{p}} \\ &\{x \in A : v(x) \geq 1\} \leftarrow v. \end{aligned}$$

(2) Let  $L/K$  be an extension of number fields, and let  $\mathfrak{p}$  be a nonzero prime ideal of  $\mathcal{O}_K$ . Show that the one-to-one correspondence of (1) for  $A = \mathcal{O}_L$  restricts to a one-to-one correspondence

$$\{\text{Prime ideals } \mathfrak{q} \text{ of } \mathcal{O}_L \text{ dividing } \mathfrak{p}\} \leftrightarrow \left\{ \begin{array}{l} \text{Normalized discrete valuations } v \text{ on } L \text{ such that} \\ v|_K = ev_{\mathfrak{p}} \text{ for some } e \in \mathbb{Z}_{\geq 1} \end{array} \right\}.$$

Here,  $v|_K$  is the restriction of  $v : L \rightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$  to  $K$  (i.e., the composition of  $v$  with the inclusion  $K \hookrightarrow L$ ).

(3) In the situation of (2), if  $\mathfrak{q}$  is a prime ideal of  $\mathcal{O}_L$  dividing  $\mathfrak{p}$ , show that  $v_{\mathfrak{q}} = e(\mathfrak{q}|\mathfrak{p})v_{\mathfrak{p}}$ .

**Question 2.** Let  $K$  be a number field, and let  $\alpha \in K^{\times}$  that is not a square in  $K$ . Consider  $L = K(\sqrt{\alpha})$ , which is a quadratic extension of  $K$ .

(1) Let  $\mathfrak{p}$  be a nonzero prime ideal of  $\mathcal{O}_K$ . If  $v_{\mathfrak{p}}(\alpha)$  is odd, show that  $\mathfrak{p}$  is ramified in  $L$ .

**Hint.** Use Question 1.

(2) Let  $\mathfrak{p}$  be a nonzero prime ideal of  $\mathcal{O}_K$  that does not divide 2. If  $v_{\mathfrak{p}}(\alpha)$  is even, show that  $\mathfrak{p}$  is unramified in  $L$ .

**Hint.** Take a uniformizer of  $\mathcal{O}_{K,\mathfrak{p}}$  to reduce to the case of  $v_{\mathfrak{p}}(\alpha) = 0$ , and use the relative discriminant.

(3) Find an example of  $K$ ,  $\alpha$ , and  $\mathfrak{p}$  (which necessarily divides 2), such that  $\mathfrak{p}$  is ramified in  $L$ , even though  $v_{\mathfrak{p}}(\alpha)$  is even.

(4) Let  $\mathfrak{p}$  be a prime ideal of  $\mathcal{O}_K$  that divides 2. If  $\alpha$  is a square modulo  $\mathfrak{p}^{2e(\mathfrak{p}|2)}$  (namely, if there exists  $x \in \mathcal{O}_K$  such that  $x^2 \equiv \alpha \pmod{\mathfrak{p}^{2e(\mathfrak{p}|2)}}$ ), show that  $\mathfrak{p}$  is unramified in  $L$ .

**Hint.** Take a uniformizer of  $\mathcal{O}_{K,\mathfrak{p}}$  to reduce to the case of  $v_{\mathfrak{p}}(\alpha) = 0$ . For  $x$  as in the problem, show that  $\frac{x+\sqrt{\alpha}}{2} \in \mathcal{O}_{K(\sqrt{\alpha}),\mathfrak{p}}$ . You need to use that  $v_{\mathfrak{p}}(4) = 2e(\mathfrak{p}|2)$ . Use Theorem 4.10 to show that  $(\mathcal{O}_K - \mathfrak{p})^{-1} \text{disc}(L/K)$  is the unit ideal of  $\mathcal{O}_{K,\mathfrak{p}}$ .

**Question 3.** Later in the course, when we learn class field theory, we will see that, for any number field  $K$ , there is a very special abelian extension  $H_K/K$ , called the **Hilbert class field of  $K$** , such that  $\text{Gal}(H_K/K) \cong \text{Cl}(K)$  and every prime ideal of  $K$  is unramified in  $H_K$ .

Although the above general fact is currently beyond our reach, in this question, we will show a very particular consequence of this general fact by hand: **for an imaginary quadratic field  $K$  with  $h_K$  even, there exists a quadratic extension  $L/K$  in which every prime ideal of  $K$  is unramified.**

Let  $K = \mathbb{Q}(\sqrt{-n})$  be an imaginary quadratic field, with  $n$  a squarefree positive integer, such that  $h_K$  is even.

- (1) Show that  $\text{disc}(K)$  has at least two prime factors.

**Hint.** Use Exercise 3.4.

- (2) Use Question 2 to show that, if  $p$  is any odd prime divisor of  $n$ , then either  $K(\sqrt{p})$  or  $K(\sqrt{-p})$  is a desired quadratic extension (i.e., where all prime ideals of  $K$  are unramified).

**Hint.** For prime ideals of  $K$  not dividing 2, use that fact that all rational prime factors of  $n$  are ramified in  $K$ . For prime ideals of  $K$  dividing 2, use the fact that either  $p$  or  $-p$  is  $1 \pmod{4}$ . Remember that such a quadratic extension exists if and only if  $h_K$  is even, so your proof must use this (e.g., Exercise 3.4) at some point.