HW #6

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Reading Homework. Try Exercises 3.1, 3.2, 3.3 in the textbook. Read its solutions in the back.

Question 1. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. We would like to show that $h_K = 1$.

(1) Use the Minkowski's bound to show that any ideal class has an integral ideal representative $\mathfrak{a}$ with $N(\mathfrak{a}) \leq 3$.

Hint. Use $K = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{5})$ to compute $\mathrm{disc}(K)$.

(2) Using how (2) factorizes in $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, show that the prime ideal factorization of (2) in K is

$$(2) = \mathfrak{q}_2^2,$$

for a unique prime ideal $\mathfrak{q}_2 \subset \mathcal{O}_K$ lying over 2. Deduce that $N(\mathfrak{q}_2) = 4$.

(3) Using how (3) factorizes in $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, show that 3 does not split completely in K. Deduce that there is no integral prime ideal of $\mathcal{O}_K$ with norm exactly equal to 3. Deduce that $h_K = 1$.

(4) In Exercise 3.2(3), it is shown that there is only one prime ideal $\mathfrak{p}_2$ of $\mathbb{Q}(\sqrt{10})$ dividing 2, and that $\mathfrak{p}_2$ is not a principal ideal. Show that this ideal generates a principal ideal over $\mathbb{Q}(\sqrt{2}, \sqrt{5})$; namely, show that $\mathfrak{p}_2\mathcal{O}_{\mathbb{Q}(\sqrt{2},\sqrt{5})}$ is a principal ideal.[1]

Question 2. Let $K = \mathbb{Q}(\sqrt{-23})$, and let $p \neq 23$ be a rational prime.

(1) Use the Minkowski's bound to show that any ideal class has an integral ideal representative $\mathfrak{a}$ with $N(\mathfrak{a}) \leq 3$.

(2) Using the factorization of the principal ideals (2), (3), $\left(\frac{1+\sqrt{-23}}{2}\right)$ and $\left(\frac{3+\sqrt{-23}}{2}\right)$, show that $h_K = 3$, with

$$\mathrm{Cl}(K) = \left\{[(1)], \left[\left(2, \frac{1+\sqrt{-23}}{2}\right)\right], \left[\left(2, \frac{-1+\sqrt{-23}}{2}\right)\right]\right\}.$$

(3) Show that p is properly represented by either $X^2 - XY + 6Y^2$, $2X^2 + XY + 3Y^2$ or $2X^2 - XY + 3Y^2$ if and only if -23 is a square mod p.

(4) Show that $p = 2X^2 \pm XY + 3Y^2$ for some $X, Y \in \mathbb{Z}$ if and only if $2p = Z^2 - ZW + 6W^2$ for some $Z, W \in \mathbb{Z}$.

(5) Combining the above, show that, for $p \neq 23$.

$$X^2 - XY + 6Y^2 \text{ represents either } p \text{ or } 2p \Leftrightarrow p \text{ is a square mod } 23.$$

[1] In fact, $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ is the **Hilbert class field** of $\mathbb{Q}(\sqrt{10})$ (one related fact is that $[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{10})] = 2 = h_{\mathbb{Q}(\sqrt{10})}$); we will see later that this is one of the properties of the Hilbert class field, that any prime ideal downstairs becomes principal in the Hilbert class field.

(6) Show that the two cases in the left side of (5) are mutually exclusive. Namely, show that there is no $p \neq 23$ such that $X^2 - XY + 6Y^2$ represents both p and $2p$.

(7) Show that, for $p \neq 23$.

$$X^2 - XY + 6Y^2 \text{ represents either } p \text{ or } 2p \Leftrightarrow X^2 + 23Y^2 \text{ represents either } 4p \text{ or } 8p.$$

(8) Show that, for $p \neq 23$,

$$X^2 + 23Y^2 \text{ represents } 4p \Leftrightarrow X^2 + 23Y^2 \text{ represents } p.$$

Hint. $n^2 \equiv 0, 1, 4 \pmod 8$.

(9) Deduce that

$$X^2 + 23Y^2 \text{ represents either } p \text{ or } 8p \Leftrightarrow p \text{ is a square mod } 23.$$

Is (8) true with $8p$ and $2p$? Namely, does $X^2 + 23Y^2$ represent $8p$ if and only if $X^2 + 23Y^2$ represents $2p$?