ZAHLENTHEORIE II – ÜBUNGSBLATT 4

PROF. DR. HÉLÈNE ESNAULT AND DR. LEI ZHANG

Exercise 1. Let $m \in \mathbb{Z}$ be a square-free integer $\neq 0, 1$, i.e. $m = \pm \prod_{i=1}^{n} p_i$, where the p_i's are distinct prime numbers and $n \geq 1$. Show that the integral closure A of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{m})$ equals

$$A = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \equiv 2 \text{ or } 3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & \text{if } m \equiv 1 \bmod 4. \end{cases}$$

Exercise 2. Consider the ring $\mathbb{Z}[\sqrt{m}]$, where m is a square free integer. Compute $\operatorname{disc}(\mathbb{Z}[\sqrt{m}]/\mathbb{Z})$ and $\operatorname{disc}(\mathcal{O}_{\mathbb{Q}[\sqrt{m}]}/\mathbb{Z})$.

Exercise 3. Use the previous exercise to understand ramification in quadratic fields.

(a) Let $m \neq 1$ be a square free integer and $K = \mathbb{Q}(\sqrt{m})$. If $p \in \mathbb{Z}$ is a prime number, we can write $p\mathcal{O}_K = (\mathfrak{p}_1 \cdot \ldots \mathfrak{p}_g)^e$ and $f = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p]$. Show that of the numbers e, f, g two are equal to 1 and one is equal to 2.

(b) We know that p ramifies in K if and only if p divides the discriminant d_K. Show that we have the following possibilities:

p **ramifies:** In this case $p|m$ or $p = 2$ and $m \equiv 2, 3 \mod 4$. We have $e = 2, f = 1, g = 1$.

p **is odd and unramified:** In this case
- $g = 2$ if and only if m is a square modulo p.
- $f = 2$ if and only if m is not a square modulo p.

$p = 2$ **and** p **is unramified:** In this case $m \equiv 1 \mod 4$ and
- $g = 2$ if and only if $m \equiv 1 \mod 8$.
- $f = 2$ if and only if $m \equiv 5 \mod 8$.

Exercise 4. Let A be the ring of integers in a number field K, and let B be the integral closure of A in a finite extension L of K. It is possible to define $\operatorname{disc}(B/A)$ as an ideal without assuming B to be a free A-module. Let $\mathfrak{p}$ be an ideal in A, and let $S = A \setminus p$. Set $B_{\mathfrak{p}} := S^{-1}B$.

(a) Show that $\operatorname{disc}(B_{\mathfrak{p}}/A_{\mathfrak{p}})$ is power of $\mathfrak{p}$. We denote the power to be $m(\mathfrak{p})$.

(b) Show that the index $m(\mathfrak{p})$ is nonzero for only finitely many $\mathfrak{p}$, and so we can define the discriminant

$$\operatorname{disc}(B/A) := \prod_{\mathfrak{p} \subseteq A} \mathfrak{p}^{m(\mathfrak{p})}$$

(c) Show that a prime ideal $\mathfrak{p}$ ramifies in B if and only if it divides $\operatorname{disc}(B/A)$.

If you want your solutions to be corrected, please hand them in just before the lecture on May 22, 2018. If you have any questions concerning these exercises you can contact Dr. Lei Zhang via `l.zhang@fu-berlin.de` or come to Arnimallee 3 112A.