ZAHLENTHEORIE II – ÜBUNGSBLATT 5

PROF. DR. HÉLÈNE ESNAULT AND DR. LEI ZHANG

Exercise 1. Let A be a Dedekind domain, $K = \mathrm{Frac}(A)$, L/K a finite separable extension and B the integral closure of A in L. Assume that there exists some $\beta \in B$ such that $B = A[\beta]$. Let $f(T) \in K[T]$ be the monic minimal polynomial of β.

(a) If $\mathfrak{p} \subseteq A$ is a prime ideal, show that there exist monic polynomials $h_1(T), \ldots, h_g(T) \in A[T]$, and $e_1, \ldots, e_g \in \mathbb{N}_{>0}$ such that
$$f(T) \equiv h_1(T)^{e_1} \cdot \ldots \cdot h_g(T)^{e_g} \mod \mathfrak{p},$$
and such that the reductions $\bar{h}_i(T) \in (A/\mathfrak{p})[T]$ are pairwise distinct and irreducible.

(b) Show that the distinct prime ideals of B lying over $\mathfrak{p}$ are given by
$$\mathfrak{P}_i := (\mathfrak{p}, h_i(\beta)), \quad i = 1, \ldots, g.$$

(c) Show that
$$\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$
and $[B/\mathfrak{P}_i : A/\mathfrak{p}] = \deg h_i$.

Exercise 2. 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 3. Let L/K be a finite Galois extension, and let A be a Dedekind domain with fraction field K. Denote B the integral closure of A in L. Now we take a prime ideal $\mathfrak{p} \subseteq A$ and two prime ideals $\mathfrak{P}$ and $\mathfrak{D}$ of B lying over $\mathfrak{p}$.

(a) Show that if $\mathfrak{D} \subseteq \cup_{1 \leq i \leq n} \mathfrak{D}_i$, and if $\mathfrak{D}_i \subseteq B$ are prime ideals, then $\mathfrak{D} = \mathfrak{D}_i$ for some i.

(b) Show that $\mathfrak{P} = \sigma(\mathfrak{D})$ for some $\sigma \in \mathrm{Gal}(L/K)$. (Hint: Otherwise $\mathfrak{D} \nsubseteq \cup_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\mathfrak{P})$. So take $d \in \mathfrak{D}$ which is not in $\cup_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\mathfrak{P})$, and consider its norm.)

If you want your solutions to be corrected, please hand them in just before the lecture on May 23, 2017. 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.